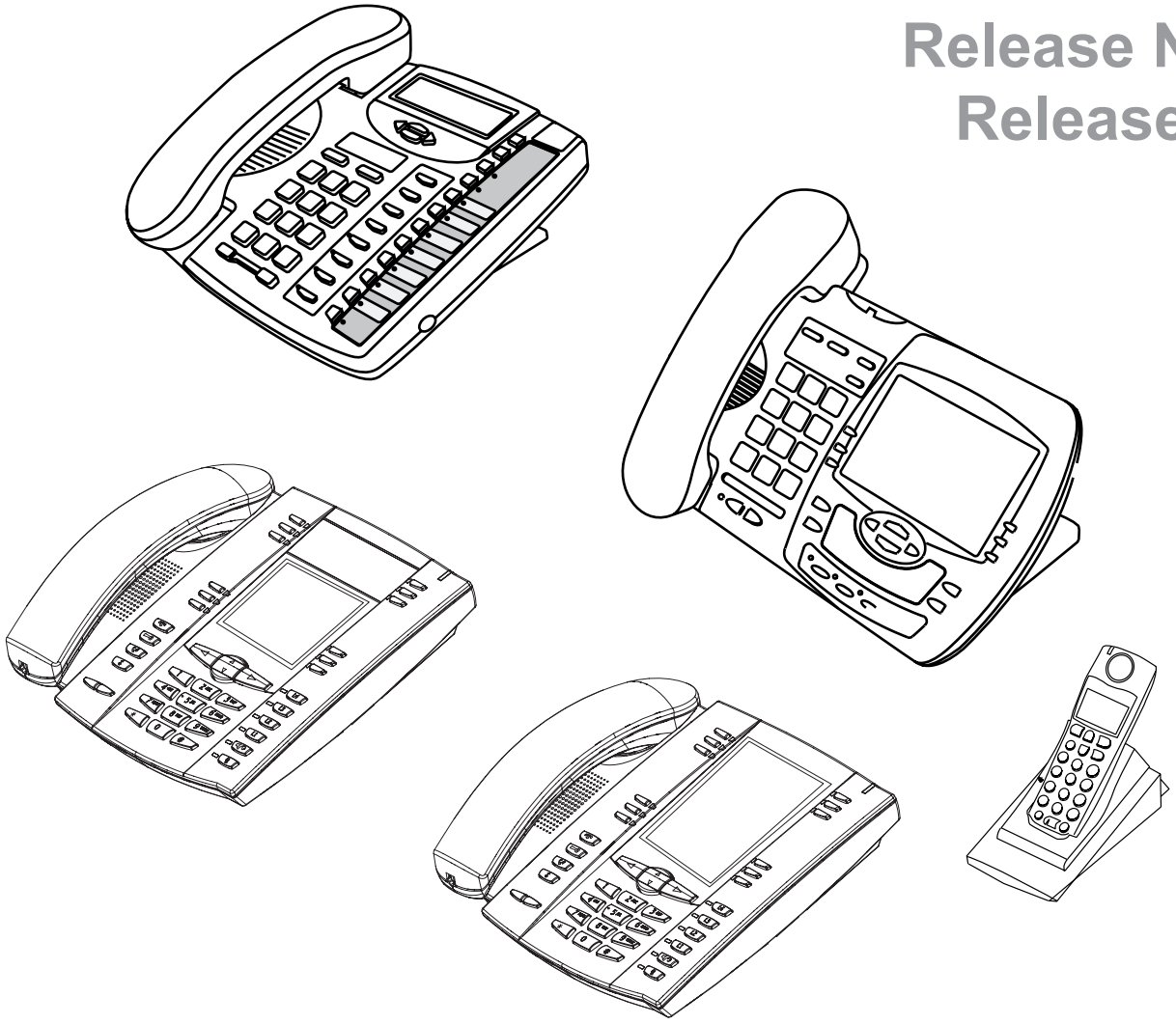
MODEL

9143i, 9480i, 9480i CT and 5i Series Phones

SIP IP PHONE

RN-001029-02
Rev 00

Release Note
Release 2.3



Downloaded from www.Manualslib.com manuals search engine

Aastra Telecom will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use. While every effort has been made to ensure accuracy, Aastra Telecom will not be liable for technical or editorial errors or omissions contained within this documentation. The information contained in this documentation is subject to change without notice.

Copyright 2008 Aastra Telecom. www.aastratelecom.com
All Rights Reserved.

Downloaded from www.Manualslib.com manuals search engine

Contents

General Information **2**
Release Content Information 2
Hardware Supported 2
Bootloader Requirements 2
Before you Upgrade **3**
Please Read Before Upgrading the Phones to Release 2.3 3
New Features in Release 2.3 ..... **4**
Description 4
Network Features 7
Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) 7
DHCP Options 159 and 160 for the Configuration Server 12
DHCP Option 12 Hostname for the Configuration Server 15
DHCP Option 77 User Class for the Configuration Server 18
Multiple DHCP Servers 21
Security Features 22
Configuration File Encryption 22
HTTPS Server Certificate Validation 23
XML Features 29
XML Execute Commands for Playing a WAV File 29
RTP Recording and Simultaneous Playing (not supported on 51i) 31
Dialpad Passthrough for Objects 34
Non-Blocking Action URI 35
New XML URI Variables 35
XML Web Applications Button 35
XML Key Redirection 36
Options Key Redirection
(for Options Menu on all phones and Services Menu on 51i) 39
XML Applications and Off-Hook Interaction 41
XML URI for Key Press Simulation 42
Using XML Commands to Reset Local Data on the Phone 45
Action URI Disconnected Feature 46
User Interface Features 49
Preferred Line Focus Feature 49
Dialpad Speeddial Supported on All Phones 52
UTF- 8 Codec for Multi-National Language Support 55
Addition of New Timezone and Country Codes 56
..... 57

Downloaded from www.Manualslib.com manuals search engine

SIP Features 57
P-Asserted-Identity (PAI) Support in UPDATE message 57
DTMF Tones in Info Requests 57
Ignore Out of Sequence Errors 58
SIP BLA Expires Timer 59
Troubleshooting Features 61
WatchDog Task Feature 61
Issues Resolved in Release 2.3 63
Contacting Aastra Telecom Support 65

Downloaded from www.Manualslib.com manuals search engine

SIP IP Phone Models 9143i, 9480i, 9480i CT and 5i Series Phones Release Note 2.3

About this Document

This Release Note 2.3 provides new features for the 5i Series IP Phones (51i, 53i, 55i, 57i, and 57i CT), and the 9143i, 9480i, and 9480i CT IP Phones. It also includes the issues resolved since Release 2.2.1 of the IP Phones.

For more detailed information about features associated with each phone, and for information on how to use the phones, see your model-specific *SIP IP Phone Installation Guide* and the *SIP IP Phone User Guide*. For detailed information about more advanced features, see the *SIP IP Phone Administrator Guide*.

Topics in this release note include:

- General Information
  (release content, hardware supported, bootloader requirements)
- New Features in Release 2.3
- Issues Resolved in Release 2.3
- Contacting Aastra Telecom Support

Downloaded from www.Manualslib.com manuals search engine

General Information

Release Content Information

This document provides release content information on the Aastra 9143i, 9480i, 9480i CT and 5i Series SIP IP phone firmware.

Model	Release Name	Release Version	Release Filename	Release Date
51i	Generic SIP	2.3.0.82	FC-001126-02-REV00	July 2008
53i	Generic SIP	2.3.0.82	FC-001086-04-REV00	July 2008
55i	Generic SIP	2.3.0.82	FC-001087-03-REV00	July 2008
57i	Generic SIP	2.3.0.82	FC-001088-03-REV00	July 2008
57i CT	Generic SIP	2.3.0.82	FC-001089-03-REV00	July 2008
9143i	Generic SIP	2.3.0.82	FC-001092-02-REV00	July 2008
9480i	Generic SIP	2.3.0.82	FC-001097-02-REV00	July 2008
9480i CT	Generic SIP	2.3.0.82	FC-001101-02-REV00	July 2008

Hardware Supported

This release of firmware is compatible with the following Aastra IP portfolio products:

- 51i
- 53i
- 55i
- 57i
- 57i CT
- 9143i
- 9480i
- 9480i CT

Bootloader Requirements

This release of firmware is compatible with the following Aastra IP portfolio product bootloader versions:

- 51i - Bootloader 2.1.0.2088 or higher
- 53i - Bootloader 2.0.1.1055 or higher
- 55i - Bootloader 2.0.1.1055 or higher
- 57i - Bootloader 2.0.1.1055 or higher
- 57i CT - Bootloader 2.0.1.1055 or higher
- 9143i - Bootloader 2.2.0.166 or higher
- 9480i - Bootloader 2.2.0.166 or higher
- 9480i CT - Bootloader 2.2.0.166 or higher

Downloaded from www.Manualslib.com manuals search engine

Before you Upgrade

Please Read Before Upgrading the Phones to Release 2.3

Release 2.3 provides several new features for the Aastra IP Phones. However, before upgrading the phones in your network to Release 2.3, please read the following IMPORTANT information:

- **In Release 2.3, LLDP is enabled by default.**
  If LLDP is enabled on your network, the phones may come up with different network settings. For more information about LLDP, see "Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)" on page 7.
- **Release 2.3 includes support for DHCP Options 159 and 160.**
  If the DHCP server supplies Options 159 and 160, the phones will attempt to contact the configuration server given in these options. For more information about Options 159 and 160, see "DHCP Options 159 and 160 for the Configuration Server" on page 12.
- **Release 2.3 provides HTTPS validation.**
  If you are using HTTPS and the certificates are not valid or are not signed by Verisign, Thawte, or GeoTrust, the phones fail to download configuration files. For more information about HTTPS validation, see "HTTPS Server Certificate Validation" on page 23.
- **Release 2.3 includes a Watchdog task feature.**
  If the phone detects a failure (for example, a crash), the phone automatically reboots. For more information about Options 159 and 160, see "WatchDog Task Feature" on page 61.

Note: If you factory default a phone with Release 2.3 software, when the phone reboots, it attempts to connect to *rcs.aastra.com*. There is no personal information transmitted from the phone and the phone continues to boot up as normal.

Downloaded from www.Manualslib.com manuals search engine

New Features in Release 2.3

Description

This section provides the new features in SIP IP Phone Release 2.3. These new features apply to all of the 5i Series phones and the 9143i, 9480i, and 9480i CT phones, unless specifically stated otherwise. Each feature also specifies whether it affects the Administrator, the User, or both.

Feature	Description
Network Features	
Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) (For Administrator)	The IP Phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).
DHCP Options 159 and 160 for the Configuration Server (For Administrator)	In addition to DHCP options 43 and 66 already supported on the IP Phones, Release 2.3 provides new DHCP Options 159 and 160.
DHCP Option 12 Hostname for the Configuration Server (For Administrator)	The IP Phones support DHCP Option 12 that the phone automatically sends to the configuration server. This option specifies the hostname (name of the client).
DHCP Option 77 User Class for the Configuration Server (For Administrator)	The IP Phones support DHCP Option 77 User Class, that is sent in DHCP request packets from the phone to the configuration server. This Option 77 defines specific User Class identifiers to convey information about a phone's software configuration or about its user's preferences.
Multiple DHCP Servers (For Administrator)	In Release 2.3, the IP Phones can now receive messages from multiple DHCP servers.
Security Features	
Configuration File Encryption (For Administrator)	Some vendors can have specific methods to encrypt files on their configuration servers. For each phone, the configuration server can generate a random hex string (encryption key) that is used to encrypt the phone's MAC-specific configuration file.
HTTPS Server Certificate Validation (For Administrator)	The HTTPS client on the IP Phones now support the validation of HTTPS certificates.
XML Features	
XML Execute Commands for Playing a WAV File (For XML Developers)	The IP Phones now allow a WAV file to be played or stopped via XML Execute commands.
RTP Recording and Simultaneous Playing (not supported on 51i) (For XML Developers)	The IP Phones allow for RTP recording and simultaneous playing of an audio file via XML Execute commands.

Downloaded from www.Manualslib.com manuals search engine

Feature	Description
Dialpad Passthrough for Objects (For XML Developers)	On the IP Phones, an XML Developer can now control digit passthrough while the phone is in the connected state using the “allowDTMF” attribute with the XML objects AastraIPPhoneTextScreen, AastraIPPhoneFormattedTextScreen, and AastraIPPhoneImageScreen.
Non-Blocking Action URI (For Administrator)	The Action URI feature on the IP Phones is now enhanced to prevent the phone from hanging if the Action URIs should fail. Also, support for transparent, non-blocking, XML post execute item URI was added.
New XML URI Variables (For Administrator and XML Developers)	Action URIs on the phone support variables, which are replaced with their corresponding value when the URI is triggered. New XML variables have been added that can be used with an onhook Action URI, and allow for enhanced information in call records and billing applications:
XML Web Applications Button (For Administrator and User)	The IP Phones now have a feature that allows a User or Administrator to access XML-based applications via a new pre-programmed softkey called, "**WebApps**".
XML Key Redirection (For XML Developers)	The IP phones now allow the redirecting of phone-based hard keys to XML scripts.
Options Key Redirection (for Options Menu on all phones and Services Menu on 51i) (For XML Developers)	The IP phones now allow the redirecting of the Options Key (Options Menu on all phones and Services Menu on the 51i) to an XML script.
XML Applications and Off-Hook Interaction (For Administrator)	In Release 2.3, a feature has been implemented that prevents the phone from going into the off-hook/dialing state when the handset is off-hook and the call ends.
XML URI for Key Press Simulation (For XML Developers)	Release 2.3 provides a feature that allows you to define XML Key URIs that can send key press events to the phone, just as if the physical hard key or softkey were pressed on the phone.
Using XML Commands to Reset Local Data on the Phone (For XML Developers)	Release 2.3 provides new XML commands that allow you to delete and reset the phone’s directory, callers list, redial list, and the local.cfg file. You use these commands with the **AastraIPPhoneExecute** object.
Action URI Disconnected Feature (For Administrator)	A new parameter, “**action uri disconnected**” has been added to Release 2.3, that allows a disconnect event to occur when the phone transitions from any active state (outgoing, incoming, connected, or calling) to an idle state.
User Interface Features	
Preferred Line Focus Feature (For Administrator & User)	In previous releases of the IP Phones, after a call (incoming or outgoing), the phone would stay on the line that was used for that call. In Release 2.3, an Administrator or User can now define a preferred line as well as a preferred timeout.

Downloaded from www.Manualslib.com manuals search engine

Feature	Description
Dialpad Speeddial Supported on All Phones (For Administrator & User)	Previously, only the 51i IP Phone supported the dialpad speeddial feature. In Release 2.3, all the phones now support this feature. Using the IP Phone UI or the Aastra Web UI, an Administrator or User can create speeddial keys on the dialpad.
UTF- 8 Codec for Multi-National Language Support (Applies to Administrator & User UIs)	The IP Phones, expansion modules, and cordless handsets previously supported ISO 8859-1 (Latin1) language. The IP Phones and expansion modules now include support for ISO 8859-2 (Latin2) of multi-national languages when displaying and inputting in the IP Phone UI and the Aastra Web UI. **Note:** UTF-8 is not applicable to the Handsets for CT models.
Addition of New Timezone and Country Codes (Administrator & User)	Five new timezone and country codes have been added to the 2.3 Release.
SIP Features	
P-Asserted-Identity (PAI) Support in UPDATE message (For Administrator)	In Release 2.3, the phones now support PAI header in the UPDATE message, according to draft-ietf-sipping-update-pai-00.
DTMF Tones in Info Requests (For Administrator)	In Release 2.3, the phones now support decoding and playing out DTMF tones sent in SIP INFO requests.
Ignore Out of Sequence Errors (For Administrator)	In Release 2.3, you can configure the phone via the "**sip accept out of order requests**" parameter to ignore CSeq number errors on all SIP dialogs on the phone.
SIP BLA Expires Timer (For Administrator)	Release 2.3 now includes a **SIP BLA subscription period** parameter that allows an Administrator to set the BLA expiration timer for how long the phone waits to receive a BLA subscribe message from the server.
Troubleshooting Features	
WatchDog Task Feature (For Administrator)	Release 2.3 provides a troubleshooting feature called the "**WatchDog**" task that monitors the status of the phones and provides the ability to get stack traces from the last time the phone failed. When the phone detects a failure (i.e., a crash), it automatically reboots.

The following paragraphs describe these features in more detail.

Downloaded from www.Manualslib.com manuals search engine

Network Features

Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)

In Release 2.3, the IP Phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED is designed to allow for things such as:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Diffserv settings) leading to "plug and play" networking.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial / asset number).

On the IP Phones, LLDP-MED performs the following:

- Supports the MAC/PHY configuration (e.g. speed rate/duplex mode).
- Supports VLAN info from the network policy; this takes precedence over manual settings.
- Allows you to enable/disable LLDP-MED if required.
- Allows you to configure time interval between successive LLDP Data Unit (LLDPDU) frames.
- Allows LLDP packets to be received from the LAN port and allows them to reach the PC Port.
- Allows the phone to use the location information, Explicit Congestion Notification (ECN) Emergency Location Identification Number (ELIN), sent by the switch, as a caller ID for making emergency calls.

Note: If the phone receives location information in ECN ELIN format (10 to 25 numeric string), the phone replaces the caller ID SIP header with the ECN ELIN value and the SIP URI does not change. The phone determines if this is an emergency number by checking the emergency dial plan configured on the phone.

You can enable or disable the LLDP-MED on the IP Phones using the configuration files, the IP Phone UI or the Aastra Web UI.

Downloaded from www.Manualslib.com manuals search engine

Configuring LLDP-MED Using the Configuration Files

Use the following parameters to configure LLDP-MED on the IP Phones.

Parameter– *lldp* *LLDP* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu->Network Settings->Ethernet&VLAN->LLDP Support Advanced Settings->Network->Advanced Network Settings
Description	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	lldp: 0	

Parameter– *lldp interval* *LLDP Packet Interval* (in Web UI)	**Configuration Files** **Aastra Web UI**	aastra.cfg, <mac>.cfg Advanced Settings->Network->Advanced Network Settings
Description	The amount of time, in seconds, between the transmission of LLDP Data Unit (LLDPDU) packets. The value of zero (0) disables this parameter.	
Format	Integer	
Default Value	30	
Range	0 to 2147483647	
Example	lldp interval: 60	

Parameter– *use lldp elin* *Use LLDP ELIN* (in Web UI)	**Configuration Files** **Aastra Web UI**	aastra.cfg, <mac>.cfg Basic Settings->Preferences->General
Description	Enables or disables the use of an Emergency Location Identification Number (ELIN) received from LLDP as a caller ID for emergency numbers.	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	use lldp elin: 0	

Downloaded from www.Manualslib.com manuals search engine

Configuring LLDP-MED Using the IP Phone UI

Use the following procedure to enable/disable LLDP-MED using the IP Phone UI.

Note: You cannot configure the "LLDP Interval" or the "Use LLDP ELIN" parameters via the IP Phone UI.

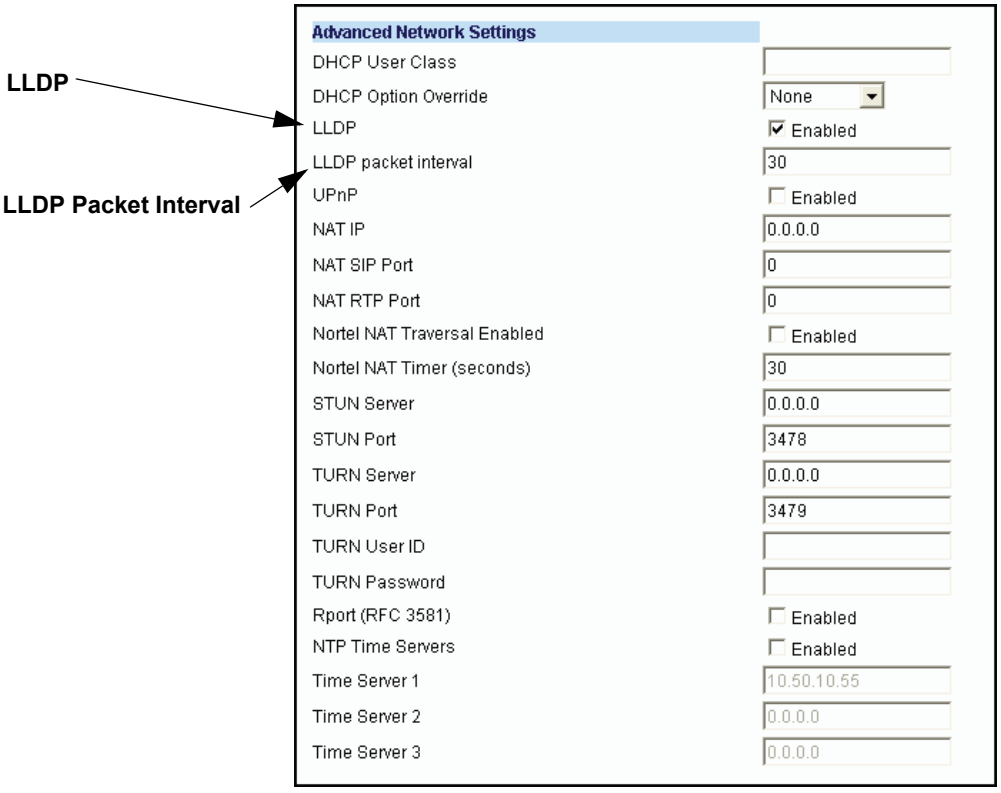
Aastra IP Phone UI

Step	Action
1	Press **Options**, and then select **Administrator Menu**. ***On the 51i:*** Press **Services,** and then select **Options->Administrator Menu**.
2	Select **Network Settings**.
3	Select **Ethernet & VLAN**.
4	Select **LLDP Support**.
5	Press **CHANGE** to toggle the LLDP setting to **Enabled** or **Disabled**. This field enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) on the IP Phone.
6	Press **DONE** to save the change.

Downloaded from www.Manualslib.com manuals search engine

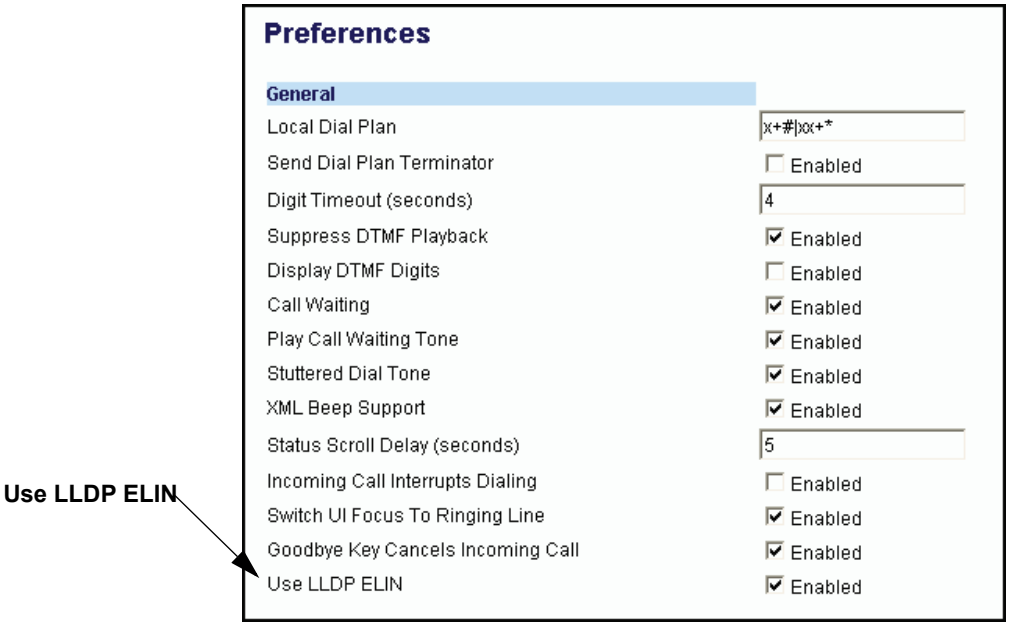
Configuring LLDP-MED Using the Aastra Web UI

Use the following procedure to configure LLDP-MED using the Aastra Web UI:

Aastra Web UI	
1	Click on **Advanced Settings->Network->Advanced Network Settings.** 
2	The "***LLDP***" field is enabled by default. To disable LLDP, click the check mark in the box to clear the check mark.
3	In the "**LLDP Packet Interval**" field, enter the time, in seconds, between the transmission of LLDP Data Unit (LLDPDU) packets. The value of zero (0) disables this parameter. Valid values are 0 to 2147483647. Default is 30.
4	Click Save Settings to save your changes.

Downloaded from www.Manualslib.com manuals search engine

Aastra Web UI

5	Select **Basic Settings->Preferences->General**. 
6	The "**Use LLDP ELIN**" field is enabled by default. To disable LLDP ELIN, click the check mark in the box to clear the check mark. This field enables or disables the use of an Emergency Location Identification Number (ELIN) received from LLDP as a caller ID for emergency numbers.
7	Click Save Settings to save your changes.

Downloaded from www.Manualslib.com manuals search engine

DHCP Options 159 and 160 for the Configuration Server

In addition to DHCP options 43 and 66 already supports on the IP Phones for setting the configuration server, Release 2.3 provides new DHCP Options 159 and 160. The IP Phones now use the following order of precedence when deriving the configuration server parameters: 43, 160, 159, 66.

In addition, an administrator can override this order of precedence by setting a configuration parameter called, **dhcp config option override.** You can set this parameter via the configuration files, IP Phone UI, or the Aastra Web UI. Setting this parameter results in the phone only using the chosen DHCP option and ignoring the other options.

Warning: Administrators should review the updated IP phone DHCP option precedence order and configuration options to avoid potential impact to existing Aastra IP phone deployments.

Configuring DHCP Option Override via the Configuration Files

Use the following parameter to configure DHCP option override on the IP Phones.

Parameter– *dhcp config option override* *DHCP Option Override* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu-> Network Settings->DHCP Settings-> Option Override Advanced Settings->Network-> Advanced Network Settings
Description	The value specified for this parameter overrides the precedence order for determining a configuration server. **Note:** You must restart the IP Phone for this parameter to take affect.	
Format	Integer	
Default Value	0 (None - no override - uses normal precedence order of 43, 160, 159, 66)	
Range	0 43 66 159 160	
Example	dhcp config option override: 66	

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCP Option Override via the IP Phone UI

Use the following procedure to configure DHCP option override via the IP Phone UI.

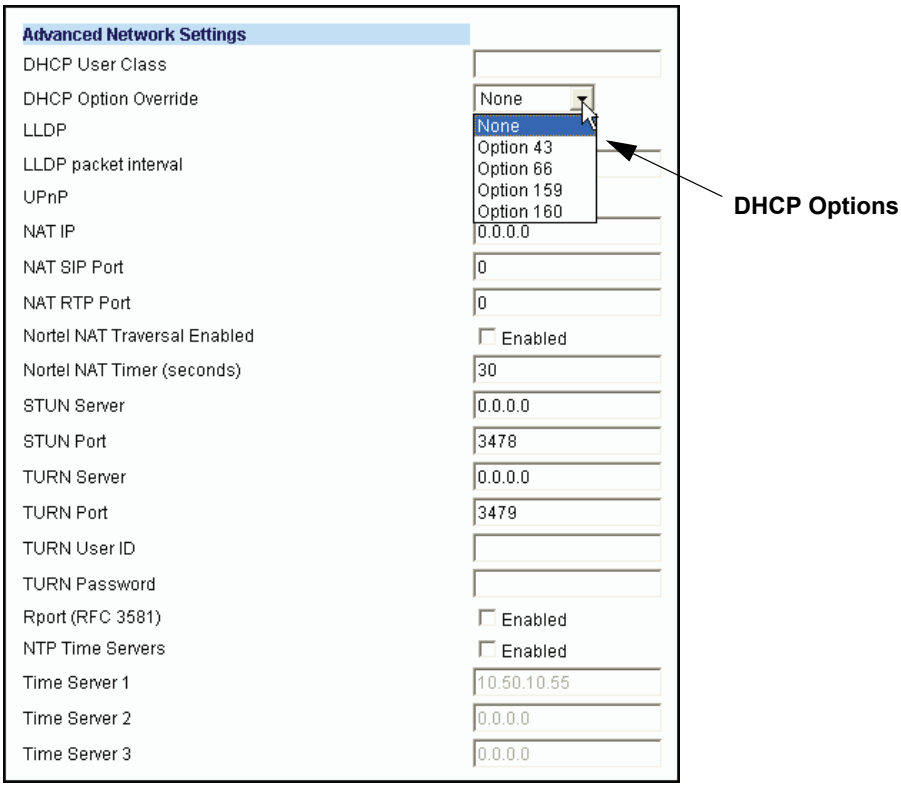
Aastra IP Phone UI

Step	Action
1	Press **Options**, and then select **Administrator Menu**. ***On the 51i:*** Press **Services,** and then select **Options->Administrator Menu**.
2	Select **Network Settings**.
3	Select **DHCP Settings**.
4	Select **Option Override**. The following list displays: • **None** (default) - no override - uses normal precedence order of 43, 160, 159, 66. • **Option 43** • **Option 66** • **Option 159** • **Option 160**
5	Choose an option that you want to use to override the DHCP normal precedence order, and press **DONE**.
6	Restart the phone for the selection to take affect.

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCP Option Override via the Aastra Web UI

Use the following procedure to configure DHCP option override using the Aastra Web UI:

Aastra Web UI	
1	Click on **Advanced Settings->Network->Advanced Network Settings.** 
2	In the "**DHCP Option Override**" field, select an option to use to override the normal precedence order. Valid values are: • **None** (default) - no override - uses normal precedence order of 43, 160, 159, 66. • **Option 43** • **Option 66** • **Option 159** • **Option 160**
3	Click Save Settings to save your changes.
4	Click on **Operation->Reset**, and restart the phone for the changes to take affect.

Downloaded from www.Manualslib.com manuals search engine

DHCP Option 12 Hostname for the Configuration Server

Release 2.3 includes a new DHCP Option 12 that the phone automatically sends to the configuration server. This option specifies the hostname (name of the client). The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character set restrictions.

Notes:

1. The hostname of [<model><MAC address>] automatically populates the field on initial startup of the phone. For example, for a 53i, the "Hostname" field is automatically populated as "53i00085D164435", where the model number is "53i" and the MAC address is "00085D164435".

2. If the configuration server sends the hostname back to the phone in a DHCP Reply Packet, the hostname is ignored.

An Administrator can change the "Hostname" for the DHCP Option 12 via the configuration files, the IP Phone UI, and the Aastra Web UI.

Changing DHCP Option 12 Hostname via the Configuration Files

Use the following parameter to change the "hostname" for DHCP Option 12.

Parameter– *hostname* *Hostname* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu->Network Settings->Hostname Advanced Settings->Network->Basic Network Settings
Description	Specifies the hostname DHCP Option 12 that the phone sends with the DHCP Request packet. **Note:** If you change this parameter, you must restart your phone for the change to take affect.	
Format	String	
Default Value	[<model><MAC IP Address>]	
Range	Up to 64 alpha-numeric characters **Note:** The value for this parameter can also be a fully qualified domain name.	
Example	hostname: aastra4	

Downloaded from www.Manualslib.com manuals search engine

Changing DHCP Option 12 Hostname via the IP Phone UI

Use the following procedure to change the “hostname” for DHCP Option 12.

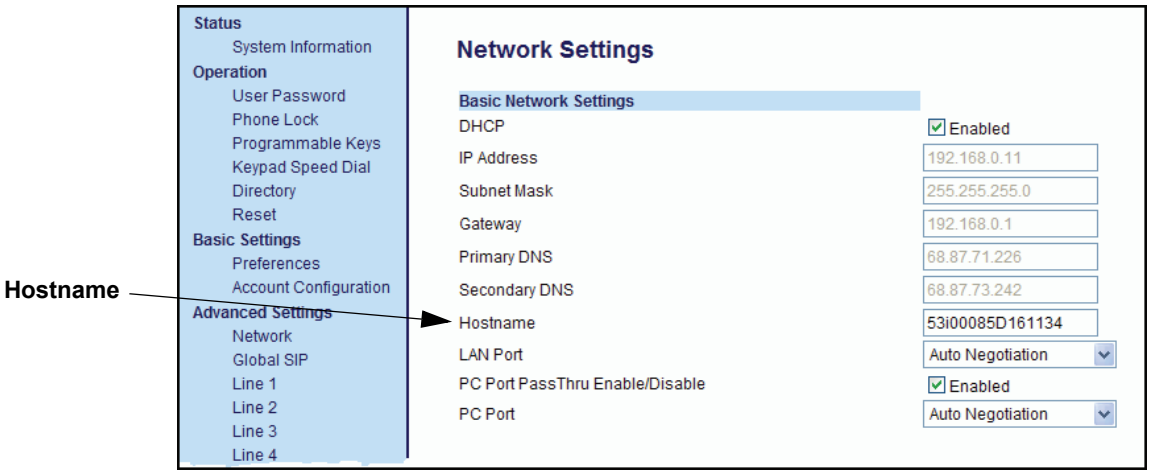
Aastra IP Phone UI

Step	Action
1	Press **Options**, and then select **Administrator Menu**. ***On the 51i:*** Press **Services,** and then select **Options->Administrator Menu**.
2	Select **Network Settings**.
3	Select **Hostname**.
4	By default, the “**Hostname**” field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435). If you want to change the hostname, enter a hostname for your phone in the “**Hostname**” field, then press **DONE**. Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
5	Restart the phone for the change to take affect.

Downloaded from www.Manualslib.com manuals search engine

Changing DHCP Option 12 Hostname via the Aastra Web UI

Use the following procedure to change the "hostname" for DHCP Option 12.

Aastra Web UI	
1	Click on **Advanced Settings->Network->Basic Network Settings.** 
2	By default, the "**Hostname**" field is automatically populated with [<Model><MAC address>] of your phone (for example, 53i00085D164435). If you want to change the hostname, enter a hostname for your phone in the "**Hostname**" field. Valid values are up to 64 alpha-numeric characters. You can use a fully qualified domain name if required.
3	Click to save your changes. **Note:** Changing the "**Hostname**" field requires a reboot of your phone.
4	Click on **Operation->Reset**, and click **RESTART**.

Downloaded from www.Manualslib.com manuals search engine

DHCP Option 77 User Class for the Configuration Server

Release 2.3 includes a new DHCP Option 77 User Class, that is sent in DHCP request packets from the phone to the configuration server. This Option 77 defines specific User Class identifiers to convey information about a phone's software configuration or about its user's preferences. For example, you can use the User Class option to configure all phones in the Accounting Department with different user preferences than the phones in the Marketing Department. A DHCP server uses the User Class option to choose the address pool for which it allocates an address from, and/or to select any other configuration option.

Notes:

1. If the User Class is not specified (left blank) in the DHCP request packet, the phone does not send the User Class DHCP Option 77.

2. Multiple User Classes inside a DHCP Option 77 are not supported.

3. DHCP Option 77 may affect the precedence of DHCP Options, dependent on the DHCP Server.

An Administrator can configure the DHCP Option 77 User Class via the configuration files, the IP Phone UI, and the Aastra Web UI.

Configuring DHCP Option 77 User Class via the Configuration Files

Use the following parameter to configure the phone to use DHCP Option 77.

Parameter– *dhcp userclass* *DHCP User Class* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu-> Network Settings->DHCP Settings-> DHCP User Class Advanced Settings->Network-> Advanced Network Settings
Description	Specifies the User Class DHCP Option 77 that the phone sends to the configuration server with the DHCP Request packet. **Note:** If you specify a value for this parameter, you must restart your phone for the change to take affect. Any change in its value during start-up results in an automatic reboot.	
Format	String	
Default Value	""	
Range	Up to 64 alpha-numeric characters	
Example	dhcp userclass: admin	

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCP Option 77 User Class via the IP Phone UI

Use the following procedure to configure the phone to use DHCP Option 77.

Aastra IP Phone UI

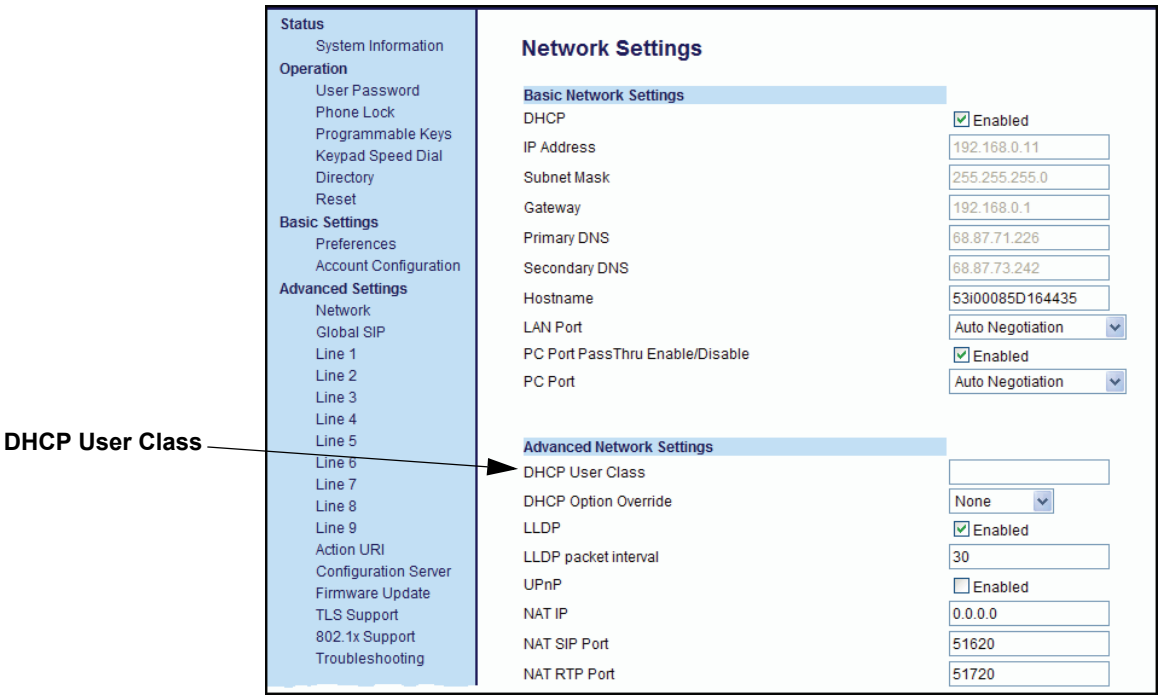
Step	Action
1	Press **Options**, and then select **Administrator Menu**. ***On the 51i:*** Press **Services,** and then select **Options->Administrator Menu**.
2	Select **Network Settings**.
3	Select **DHCP Settings**.
4	Select **DHCP User Class**.
5	In the "**DHCP User Class**" field, enter a DHCP User Class to apply to your phones, then press **DONE**. Valid values are up to 64 alpha-numeric characters. For example, "**admin**".
6	Restart the phone for the change to take affect.

Downloaded from www.Manualslib.com manuals search engine

Configuring DHCP Option 77 User Class via the Aastra Web UI

Use the following procedure to configure the phone to use DHCP Option 77.

Aastra Web UI

1	Click on **Advanced Settings->Network->Advanced Network Settings.** 
2	In the “**DHCP User Class**” field, enter a DHCP User Class to apply to your phones. For example, “**admin**”. Valid values are up to 64 alpha-numeric characters.
3	Click Save Settings to save your changes. **Note:** Entering a value in the “**DHCP User Class**” field requires a reboot of your phone.
4	Click on **Operation->Reset**, and click **RESTART**.

Downloaded from www.Manualslib.com manuals search engine

Multiple DHCP Servers

In Release 2.3, the IP Phones can now receive messages from multiple DHCP servers.

After the phone receives its first DHCP message, it listens for a specific time period, for more DHCP messages. If the first DHCP offer contains configuration server information (Options 43, 66, 159 or 160), then the phone times out and continues using the first DHCP offer, without listening for more DHCP offers. If the first DHCP message contains no configuration server information, the phone continues to listen for other DHCP messages. If the second DHCP message contains configuration server information and other conditions, the phone chooses the second DHCP message over the initial DHCP message.

Note: If the **DHCP Option Override** parameter is enabled with a value (Option 43, Option 66, Option 159, or Option 160), the phone checks the override option setting before timing out.

IMPORTANT NOTE

Users currently using multiple DHCP servers on a single network could be affected by this new feature.

Downloaded from www.Manualslib.com manuals search engine

Security Features

Configuration File Encryption

Some vendors can have specific methods to encrypt files on their configuration servers. For each phone, the configuration server can generate a random hex string (encryption key) that is used to encrypt the phone's MAC-specific configuration file.

The encryption key is placed in a plain text MAC-specific configuration file that the server downloads to the phone. After the phone receives the file, it updates the encryption key.

This method of encryption does not affect the implementation of the Aastra method of file encryption.

Note: The *aastra.cfg* file is not encrypted with this feature.

You can set the phone-specific encryption key using the configuration files only.

For more information about configuration file encryption, contact Aastra Technical Support.

Configuring Configuration File Encryption

Use the following parameter to configure configuration file encryption on the IP Phones.

Parameter– *config encryption key*	**Configuration Files** aastra.cfg, <mac>.cfg
Description	Specifies the phone-specific encryption key that the configuration server uses to encrypt in a MAC-specific configuration file.
Format	String
Default Value	Not applicable
Range	String length of 4 to 32 alphanumeric characters
Example	config encryption key: 123abcd

Downloaded from www.Manualslib.com manuals search engine

HTTPS Server Certificate Validation

The HTTPS client on the IP Phones now support validation of HTTPS certificates. This new feature supports the following:

- Verisign, GeoTrust, and Thawte signed certificates
- User-provided certificates
- Checking of hostnames
- Checking of certificate expiration
- Ability to disable any or all of the validation steps
- Phone displays a message when a certificate is rejected (except on check-sync operations)

All validation options are enabled by default.

Certificate Management

Aastra Provided Certificates

The phone comes with root certificates from Verisign, GeoTrust, and Thawte pre-loaded.

User Provided Certificates

The administrator has the option to upload their own certificates onto the phone. The phone downloads these certificates in a file of .PEM format during boot time after configuration downloads. The user-provided certificates are saved on the phone between firmware upgrades but are deleted during a factory default. The download of the User-provided certificates are based on a filename specified in the configuration parameter, **https user certificates** (**Trusted Certificates Filename** in the Aastra Web UI; User-provided certificates are not configurable via the IP Phone UI).

Note: Certificates that are signed by providers other than Verisign, GeoTrust or Thwate do not verify on the phone by default. The user can overcome this by adding the root certificate of their certificate provider to the use-provided certificate .PEM file.

Downloaded from www.Manualslib.com manuals search engine

Certificate Validation

Certificate validation is enabled by default. Validation occurs by checking that the certificates are well formed and signed by one of the certificates in the trusted certificate set. It then checks the expiration date on the certificate, and finally, compares the name in the certificate with the address for which it was connected.

If any of these validation steps fail, the connection is rejected. Certificate validation is controlled by three parameters which you can configure via the configuration files, the IP Phone UI, or the Aastra Web UI:

- **https validate certificates** - Enables/disables validation
- **https validate hostname** - Enables/disables the checking of the certificate commonName against the server name.
- **https validate expires** - Enables/disables the checking of the expiration date on the certificate.

User Interface

Certificate Rejection

When the phone rejects a certificate, it displays, ***"Bad Certificate"*** on the LCD.

Configuring HTTPS Server Certificate Validation via the Configuration Files

Use the following parameters to configure HTTPS server certificate validation for the IP Phones using the configuration files.

Parameter– *https validate certificates* *Validate Certificates* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu-> Configuration Server->HTTPS Settings-> Cert Validation->Enable Advanced Settings->Network->HTTPS Settings
Description	Enables or disables the HTTPS validation of certificates on the phone. When this parameter is set to 1, the HTTPS client performs validation on SSL certificates before accepting them. **Note: If you are using HTTPS as a configuration method, and use a self signed certificate, you must set this parameter to "0" (disabled) before upgrading to Release 2.3 of the IP Phones.**	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	https validate certificates: 0	

Downloaded from www.Manualslib.com manuals search engine

Parameter– *https validate expires* *Check Certificate Expiration* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu-> Configuration Server->HTTPS Settings-> Cert Validation->Check Expires Advanced Settings->Network->HTTPS Settings
Description	Enables or disables the HTTPS validation of the expiration of the certificates. When this parameter is set to 1, the HTTPS client verifies whether or not a certificate has expired prior to accepting the certificate. **Note:** If the "**https validate expires**" parameter is set to **enable**, the clock on the phone must be set for the phone to accept the certificates.	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	https validate expires: 0	

Parameter– *https validate hostnames* *Check Certificate Hostnames* (in Web UI)	**Configuration Files** **IP Phone UI** **Aastra Web UI**	aastra.cfg, <mac>.cfg Options->Administrator Menu-> Configuration Server->HTTPS Settings-> Cert Validation->Check Hostnames Advanced Settings->Network->HTTPS Settings
Description	Enables or disables the HTTPS validation of hostnames on the phone.	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	https validate hostnames: 0	

Parameter– *https user certificates* *Trusted Certificates Filename* (in Web UI)	**Configuration Files** **Aastra Web UI**	aastra.cfg, <mac>.cfg Advanced Settings->Network->HTTPS Settings
Description	Specifies a file name for a .PEM file located on the configuration server. This file contains the User-provided certificates in PEM format. These certificates are used to validate peer certificates. **Note:** You must disable the "**https validate certificates**" parameter in order for the phone to accept the User-provided certificates.	
Format	Alphanumeric string in the format <filename.pem>	
Default Value	Not applicable	
Range	Not applicable	
Example	https user certificates: trustedCerts.pem	

Downloaded from www.Manualslib.com manuals search engine

Configuring HTTPS Server Certificate Validation via the IP Phone UI

Use the following procedure to configure HTTPS server certificate validation for the IP Phones using the IP Phone UI.

Aastra IP Phone UI

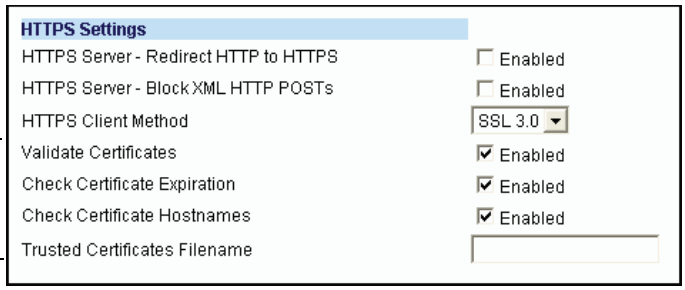
Step	Action
1	Press **Options**, and then select **Administrator Menu**. ***On the 51i:*** Press **Services,** and then select **Options->Administrator Menu**.
2	Select **Configuration Server**.
3	Select **HTTPS Settings->Cert. Validation**. The following list displays: • **Enable** • **Check Expires** • **Check Hostnames**
Enable/Disable HTTPS Server Certificate Validation	
4	Select **Enable**.
5	Press **Change** to toggle the **"Enable"** field to **"Yes" or "No".** **Note:** If you are using HTTPS as a configuration method, and use a self signed certificate, you must set this field to "**No**" before upgrading to Release 2.3 of the IP Phones.
6	Press **DONE** to save the change and return to the Certificates screen. **Note:** This change is immediately applied after pressing **DONE**.
Enable/Disable HTTPS Validate Certificate Expiration	
7	Select **Check Expires**.
8	Press **Change** to toggle the **"Check Expires"** field to **"Yes" or "No".** **Notes**: **1.** This change is immediately applied after pressing **DONE**. **2.** If the "**Check Expires**" parameter is set to **Yes**, the clock on the phone must be set for the phone to accept the certificates.
9	Press **DONE** to save the change and return to the Certificates screen. **Note:** This change is immediately applied after pressing **DONE**.
Enable/Disable HTTPS Validate Hostnames	
10	Select **Check Hostnames**.
11	Press **Change** to toggle the **"Check Hostnames"** field to **"Yes" or "No".**

Downloaded from www.Manualslib.com manuals search engine

Aastra IP Phone UI	
Step	**Action**
12	Press **DONE** to save the change and return to the Certificates screen. **Note:** This change is immediately applied after pressing **DONE**.
13	Press to exit the Options Menu and return to the idle screen.

Configuring HTTPS Server Certificate Validation via the Aastra Web UI

Use the following procedure to configure HTTPS server certificate validation for the IP Phones using the Aastra Web UI.

Aastra Web UI	
1	Click on **Advanced Settings->Network->HTTPS Settings.** **HTTPS Validation Certificate Parameters** 
2	The **"Validate Certificates"** field is enabled by default. To disable validation of certificates, click the check mark in the box to clear the check mark. When this parameter is enabled, the HTTPS client performs validation on SSL certificates before accepting them. **Notes**: **1.** This parameter is immediately applied after clicking the **SAVE SETTINGS** button. **2. If you are using HTTPS as a configuration method, and use a self signed certificate, you must disable (uncheck) this field before upgrading to Release 2.3 of the IP Phones**.
3	The **"Check Certificate Expiration**" field is enabled by default. To disable validation of certificate expiration, click the check mark in the box to clear the check mark. When this parameter is enabled, the HTTPS client verifies whether or not a certificate has expired prior to accepting the certificate. **Notes**: **1.** This parameter is immediately applied after clicking the **SAVE SETTINGS** button. **2.** If the "**Check Certificates Expiration**" parameter is set to **Yes**, the clock on the phone must be set for the phone to accept the certificates.

Downloaded from www.Manualslib.com manuals search engine

Aastra Web UI	
4	The **"Check Certificate Hostnames**" field is enabled by default. To disable validation of hostnames, click the check mark in the box to clear the check mark. **Note:** This parameter is immediately applied after clicking the **SAVE SETTINGS** button.
5	If you require the download of User-provided certificates in a .PEM formatted file, enter the file name in the format <filename.pem> in the "**Trusted Certificates Filename**" field. For example: **trustedCerts.pem** This parameter specifies a file name for a .PEM file located on the configuration server. This file contains the User-provided certificates in PEM format. These certificates are used to validate peer certificates. **Notes**: **1.** You must disable the "**Validate Certificates**" field in order for the phone to accept the User-provided certificates. **2.** This parameter requires you restart the phone in order for it to take affect.
6	Click Save Settings to save your changes.
7	If you entered a filename in the "**Trusted Certificates Filename**" field, click on **Operation->Reset**, and restart the phone for the changes to take affect.

Downloaded from www.Manualslib.com manuals search engine

XML Features

XML Execute Commands for Playing a WAV File

The IP Phones now allow a WAV file to be played or stopped via XML Execute commands. A WAV file is an audio file format standard for storing an audio bit stream on a system in raw, uncompressed format or compressed format to reduce the file size.

A WAV file can be streamed to the phone using the HTTP protocol.

The WAV feature supports the following:

- Streaming of the WAV file to allow it to be locally played
- Allows you to abort the audio streaming by pressing the **Goodbye** key on the phone.
- Supports the HTTP file download protocol
- Supports the aLaw and uLaw codecs
- Calls "**Action URI INCOMING**" when the audio WAV starts, and "**Action URI ONHOOK**" when the WAV file playing has completed. The name of the WAV file is inserted into the Action URI.
- Plays the WAV file only if the phone is idle.
- Aborts streaming if another line is selected for dialing out, or if the current line is accepting an incoming call.
- WAV audio file starts only when 4 seconds of the audio data (or the complete file) has been accumulated.
- Follows the standard phone behavior of speaker/head set/hand set.

An Administrator can use two new XML Execute commands with the AastraIPPhoneExecute object to allow the phones to play a WAV file:

- **Wav.Play** - This command initiates the streaming of a WAV file to the phone.
- **Wav.Stop** - This command aborts a WAV streaming.

Downloaded from www.Manualslib.com manuals search engine

XML Command: Wav.Play

The **Wav.Play** XML Execute command starts the streaming of a WAV file. You enter this command with the AastraIPPhoneExecute object in the following format:

`Wav.Play:http://[username[:password]@]<host>[/<path>]/<file>`

The following are examples of using the wav.play command with the XML Execute object.

Examples

```
<AastraIPPhoneExecute>
<ExecuteItem URI="Wav.Play:http://10.30.101.26/wavfiles/example.wav" />
<AastraIPPhoneExecute>
```

```
<AastraIPPhoneExecute>
  <ExecuteItem URI="Wav.Play:http://user:password@10.30.101.26/example.wav" />
<AastraIPPhoneExecute>
```

XML Command: Wav.Stop

The **Wav.Stop** Execute command aborts a WAV streaming currently in progress. You enter this command with the AastraIPPhoneExecute object in the following format:

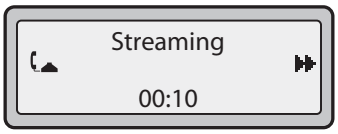
`Wav.Stop:`

Example

```
<AastraIPPhoneExecute>
    <ExecuteItem URI="Wav.Stop:" />
<AastraIPPhoneExecute>
```

IP Phone UI Screens During WAV Streaming

The 9143i, 51i, and 53i LCD screens display the following during WAV streaming.



The 9480i, 9480i CT, 55i, 57i, and 57i CT screens display the following during WAV streaming.

Downloaded from www.Manualslib.com manuals search engine

To abort the WAV streaming, a user can press any of the following:

- **Goodbye** key
- **Drop** softkey
- **Line** key (not applicable to the 51i)

You can also place the handset (if in use) on hook.

RTP Recording and Simultaneous Playing (not supported on 51i)

The IP Phones now allow for RTP recording and simultaneous playing of an audio file via XML Execute commands. An Administrator can use the RTP and multicast RTP commands (RTPTx, RTPRx, RTPMTx, RTPMRx) with the "**AastraIPPhoneExecute**" object to initiate this feature.

The RTP and multicast RTP commands allow the phone to send/receive an RTP stream to/from given multicast/unicast addresses (without involving SIP signaling). An Administrator can use the following two options appended to the RTP commands for recording and simultaneously playing of an audio file:

- **mix** - When appended to an RTP command, "**mix**" enables RTP recording and simultaneous playing of an audio file.
- **disableIcon** - When appended to an RTP command, "**disableIcon**" disables the display of the mixed call icons on the LCD of the phones.

Note: This feature is not supported on the 51i. Also, if the cordless handset (CT) and the base phone are connected (Models 9480i CT and 57i CT), this feature is not supported.

Sending RTP

When a phone receives a request for sending RTP:

- and there is an existing call on the phone, no new audio session is created; the existing RTP call (incoming or outgoing) is sent to the receiving party.
- and the phone is already in a 3-way conference, the request is declined.
- and there is no existing call on the phone, a new audio session is created and the RTP call is sent to the receiving party.

The following scenarios assume that a request for sending mixed RTP is initiated.

Phone State	Action When RTP Transmitting
Phone is in idle state.	The phone initiates a new RTP session on the paging line and the paging line displays.
There is an existing voice call on the phone.	The phone starts sending the mixed RTP stream, paging line does not display.
The phone is in conference.	The request for sending RTP is declined.
The phone is not in conference; however, both voice and conference streams are busy (cordless handset).	The request for sending RTP is declined.

Downloaded from www.Manualslib.com manuals search engine

Phone State	Action When RTP Transmitting
The phone is in a call using the conference stream and the voice stream is free.	Paging call is initiated using the voice stream with the mixed audio from the conference stream; paging line does not display.
The active voice call is dropped. (Mixed RTP stream was being sent using this voice call).	RTP stream is dropped.
A new call comes in while an active voice call is put on hold. (Mixed RTP stream was being sent using this voice call).	RTP mixed stream is sent for the currently active call.
The phone is sending the mixed RTP stream, and there is an existing voice call on the phone. A request for initiating localized conference is initiated.	Localized conference request is declined, and the focus is given back to the initiating line.

Note: When an RTP stream is being sent with RTP recording and simultaneous playing (mix), the IP Phone LCD displays an icon with an '**m**' on top to indicate that a mixed RTP stream is being sent.

Downloaded from www.Manualslib.com manuals search engine

Receiving RTP

When a phone receives a request for receiving RTP:

- if there is an existing audio path, (handset, headset, or speakerphone), the phone uses it to play the incoming RTP stream on top of the existing one.
- if the phone is already in a 3-way conference, the request is declined.
- if there is no existing audio path, the phone creates a new one (speakerphone) to play the incoming RTP stream

The following scenarios assume that a request for receiving mixed RTP is initiated.

Phone State	Action When RTP Receiving
Phone is in idle state.	The phone initiates a new RTP session on the paging line and the paging line displays.
There is an existing voice call on the phone.	The phone starts playing the incoming RTP stream on top of the existing call. Paging line does not display.
The phone is in conference.	The request for receiving RTP is declined.
The phone is not in conference; however, both voice and conference streams are busy (cordless handset).	The request for receiving RTP is declined.
The phone is in a call using the conference stream and the voice stream is free.	Incoming RTP stream is played on top of the existing voice stream. Paging line does not display.
The active voice call is dropped. (RTP stream was being played on top of this voice call).	RTP stream is dropped.
A new call comes in while an active voice call is put on hold. (RTP stream was being played on top of this voice call).	RTP mixed stream is played on top of the currently active call.
The active voice call is dropped	RTP stream is dropped.

Note: When RTP stream is being received with RTP recording and simultaneous playing (mix), you can use the volume controls on the IP phone to adjust the volume (increase or decrease) to your specifications.

Downloaded from www.Manualslib.com manuals search engine

Examples

The following are examples of using the "**mix**" and "**disableIcon**" execute commands with the **AastraIPPhoneExecute** object. These commands apply to both the RTP and multicast RTP XML commands (RTPTx, RTPRx, RTPMTx, RTPMRx).

- Send mix unicast RTP stream (if there is existing voice call) to 10.30.100.20:21000. Mix icon is displayed on the phone's call screen.

```
<AastraIPPhoneExecute>
   <ExecuteItem URI="RTPTx:10.30.100.20:21000:mix">
</AastraIPPhoneExecute>
```

- Receive unicast RTP stream from 10.30.100.20 at port 21000 with the egress voice settings at 3 levels more than the current offset and play on top of the existing voice stream (if any).

```
<AastraIPPhoneExecute>
   <ExecuteItem URI="RTPRx:10.30.100.20:21000:3:mix">
</AastraIPPhoneExecute>
```

- Receive unicast RTP stream from 10.30.100.20 at port 21000 with the voice settings as used earlier and play on top of the existing voice call (if any). Also, the mixing icon is not shown on the call screen.

```
<AastraIPPhoneExecute>
   <ExecuteItem URI="RTPRx:10.30.100.20:21000:mix:disableIcon">
</AastraIPPhoneExecute>
```

Dialpad Passthrough for Objects

In previous releases, when an XML application was active on the phone, it suppressed all dialpad events. This suppression was to prevent digit events from being sent to the underlying line application.

On the IP Phones, an XML Developer can now control digit passthrough while the phone is in the connected state. (This feature is only applicable to phones in the connected state). This can be done by setting the new "**allowDTMF**" attribute with the XML objects **AastraIPPhoneTextScreen**, **AastraIPPhoneFormattedTextScreen**, and **AastraIPPhoneImageScreen**. Setting this attribute to "**yes**" allows dialpad events to pass through the XML applications.

Note: The default behavior for this feature is to suppress dialpad events when an XML object is in focus (same as in previous releases). Other XML objects ignore this attribute.

Downloaded from www.Manualslib.com manuals search engine

Examples

- The following is an example of setting the **allowDTMF** attribute to allow dialpad events to pass through the XML applications.

```
<AastraIPPhoneTextScreen allowDTMF="yes">
   <Title>Test</Title>
   <Text>Digits should pass through this object</Text>
</AastraIPPhoneTextScreen>
```

- The following is an example of setting the **allowDTMF** attribute to prevent dialpad events from passing through the XML applications (this is the default setting).

```
<AastraIPPhoneTextScreen allowDTMF="no">
   <Title>Test</Title>
   <Text>Digits do not pass through this object</Text>
</AastraIPPhoneTextScreen>
```

Non-Blocking Action URI

The Action URI feature on the IP Phones is now enhanced to prevent the phone from hanging if the Action URIs should fail. Also, support for transparent, non-blocking, XML post execute item URI was added.

New XML URI Variables

Action URIs on the phone support variables, which are replaced with their corresponding value when the URI is triggered. New XML variables have been added that can be used with an onhook Action URI, and allow for enhanced information in call records and billing applications:

- **$$LOCALIP$$** - Phone's IP address
- **$$CALLDURATION$$** - Duration of the current/last call
- **$$CALLDIRECTION$$** - Specifies whether the current/last call was incoming or outgoing

XML Web Applications Button

The IP Phones now have a feature that allows a User or Administrator to access XML-based applications via a new pre-programmed softkey called, "**WebApps**".

On the 55i, 57i, 57i CT, 9480i, and 9480i CT phones, the WebApps softkey displays on softkey 1 on the idle screen.

On the 51i, 53i, and 9143i, you can access the WebApps option in the Services menu.

You can set any programmable or softkey as a WebApps key. Pressing this key redirects the phone to a Web application provided by your Administrator.

Downloaded from www.Manualslib.com manuals search engine

XML Key Redirection

The IP phones now allow the redirecting of phone-based hard keys to XML scripts. This allows the server to provide the phone with Redial, Transfer (Xfer), Conference (Conf), and Intercom (Icom) key features, and the Voicemail option feature, rather then accessing them from the phone-side. This feature allows you to access the redirected keys and voicemail option from the server using the IP Phone's Services Menu. By default, the server-side keys function the same as the phone-side key features.

The following table identifies the phone states that apply to each key redirection.

Hard Keys/Options	Redirects in
Conference (Conf)	the connected state
Transfer (Xfer)	the connected and dialing states
Redial	all states
Intercom (Icom)	all states
Voicemail	all states

Notes:
1. If XML key redirection is enabled on the 51i., the **Xfer** and **Conf** menu items perform redirection.
2. Key remapping takes precedence over redirecting.
3. Disabling the redial, conference, or transfer features on the phone also disables the redirection of these keys.

The following URI configuration parameters control the redirection of the keys and the voicemail option:

- **redial script**
- **xfer script**
- **conf script**
- **icom script**
- **voicemail script**

An Administrator can configure the XML key, redirection URI parameters using the configuration files only.

Downloaded from www.Manualslib.com manuals search engine

Configuring XML Redirection of the Redial, Xfer, Conf, and Icom Keys, and the Voicemail Option

Use the following script parameters to redirection the Redial, Xfer, Conf, and Icom keys, and the Voicemail Option so that these features are provided by the server instead of the phone.

Parameter–*redial script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies a redial script for the phone to use. When this parameter is set, pressing the Redial key GETs the specified URI from the server to use in performing the redial action.
Format	String
Default Value	empty
Range	Any valid URI
Example	redial script: http://bluevelvet.ana.aastra.com/redial.php

Parameter–*xfer script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies an Xfer script for the phone to use. When this parameter is set, pressing the Xfer key GETs the specified URI from the server instead of starting the transfer action.
Format	String
Default Value	empty
Range	Any valid URI
Example	xfer script: http://bluevelvet.ana.aastra.com/xfer.php

Parameter–*conf script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies an Conf script for the phone to use. When this parameter is set, pressing the Conf key GETs the specified URI from the server to use in performing the conference action.
Format	String
Default Value	empty
Range	Any valid URI
Example	conf script: http://bluevelvet.ana.aastra.com/conf.php

Downloaded from www.Manualslib.com manuals search engine

Parameter–*icom script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies an Icom script for the phone to use. When this parameter is set, pressing the Icom key GETs the specified URI from the server to use in performing the Intercom action.
Format	String
Default Value	empty
Range	Any valid URI
Example	icom script: http://bluevelvet.ana.aastra.com/icom.php

Parameter–*voicemail script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies an Voicemail script for the phone to use. When this parameter is set, selecting the voicemail option from the Services Menu GETs the specified URI from the server instead of starting the Voicemail application.
Format	String
Default Value	empty
Range	Any valid URI
Example	voicemail script: http://bluevelvet.ana.aastra.com/voicemail.php

Downloaded from www.Manualslib.com manuals search engine

Options Key Redirection
(for Options Menu on all phones and Services Menu on 51i)

The IP phones now allow the redirecting of the Options Key (Options Menu on all phones and Services Menu on the 51i) to an XML script. This allows the server to provide the phone with available options, rather then accessing them from the phone-side. You access the Options Key XML script by pressing the Options Key. You can still access the Options Menu from the phone-side by pressing and holding the Options key to display the phone-side Options Menu.

The following URI configuration parameter controls the redirection of the Options Key:

- **options script**

IMPORTANT NOTES

- If no Options URI script is configured, the local Options Menu on the phone displays as normal.
- If you configure password access to the Options Menu, this password is required when accessing the local Option Menu, but is not required for the Options Key redirection feature.
- Pressing the Options Menu for redirection from the server does not interfere with normal operations of the phone (for example, pressing the options menu when on a call does not affect the call).
- If the phone is locked, you must unlock the phone before accessing the Options Menu redirect feature. After pressing the Options Key, the phone displays a screen that allows you to unlock the phone before continuing.
- On the 51i, the redirection feature works after selecting “Options” from the Services Menu. To display the original Options Menu, press and hold the Services key.

An Administrator can configure the XML Options Key (or Services Key on the 51i), redirection URI parameter using the configuration files only.

Downloaded from www.Manualslib.com manuals search engine

Configuring XML Redirection of the Options Key (Services Key on the 51i)

Use the following parameter to configure XML redirection of the Options Key (or Services Key on the 51i).

Parameter– *options script*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies an Options script for the phone to use. When this parameter is set, pressing the Options Key (or Services Key on the 51i) GETs the specified URI from the server. **Note:** Pressing and holding the Options key (or the Services Key on the 51i) displays the local Options Menu on the phone.
Format	String
Default Value	empty
Range	Any valid URI
Example	options script: http://fargo.ana.aastra.com/options.xml

Downloaded from www.Manualslib.com manuals search engine

XML Applications and Off-Hook Interaction

In Release 2.3, a feature has been implemented that prevents the phone from going into the off-hook/dialing state when the handset is off-hook and the call ends.

In previous releases, the phone behaved as in the following scenario:

You are in a call using the handset and the phone displays an XML application. The far-end terminates the call, and a new XML application gets pushed/pulled onto the display. Since the handset is off-hook and in idle mode, the "offhook idle timer" starts. When this timer expires, the phone applies dial tone and moves to the off-hook/dialing state, which then destroys the XML application that was being displayed.

In Release 2.3, you can set an "**auto offhook**" parameter that determines whether or not the phone is prevented from entering the off-hook/dialing state, if the handset is off-hook and the call ends.

An Administrator can enable or disable the "**auto offhook**" parameter using the configuration files only.

Configuring the Off-Hook Interaction Feature

Use the following parameter to configure the XML application and off-hook interaction feature.

Parameter– *auto offhook*	**Configuration Files**aastra.cfg, <mac>.cfg
Description	Specifies whether or not the phone is prevented from entering the off-hook/ dialing state, if the handset is off-hook for more than 2 seconds, and the call ends.
Format	Boolean
Default Value	0 (disabled)
Range	0 (disabled) 1 (enabled)
Example	auto offhook: 1

Downloaded from www.Manualslib.com manuals search engine

XML URI for Key Press Simulation

Release 2.3 provides a feature that allows an XML Developer or Administrator to define XML Key URIs that can send key press events to the phone, just as if the physical hard key, softkey, or programmable key were pressed on the phone.

When the Key URI event is sent from the server to the phone, the phone initiates the event as if the key was physically pressed. If the key is not present on the phone (hard key) or not available (softkey or programmable key), when the phone receives the URI, the event is discarded. If you are in the process of changing the softkey or programmable key setting, or the key is disabled while the event is being processed, the request is discarded. The phone maps key events to it's physical keys and not to it's mapped logical keys.

The following table identifies the XML URIs for pressing buttons on the phone..

XML Key URI	Description
Line Keys	
Key:Line1 to Key:Line4	Line 1 to 4 Keys **Note:** The phone ignores URI line keys 5 to 9 since it does not have Line 5 to 9 physical keys.
Keypad Keys	
Key:KeyPad0 to Key:KeyPad9	Numeric Keypad Keys 0-9
Key:KeyPadStar	* - Star Key
Key:KeyPadPound	# Hash Key
Softkeys	
Key:SoftKey1 to Key:SoftKey<n>	Softkey 1 to <n> (valid softkeys depend on the number of physical softkeys on the phone)
Key:TopSoftKey1 to Key:TopSoftKey<n> top	Top softkeys 1 to <n> ((valid top softkeys depend on the number of physical top softkeys on the phone)
Programmable Keys	
Key:PrgKey1 to Key:PrgKey<n>	Programmable keys 1 to <n> (valid programmable keys depend on the number of physical programmable keys on the phone)
Expansion Module Keys	
Key:ExpMod1SoftKey1 to Key:ExpMod1SoftKey60	Expansion module 1 softkeys 1 to 60 **Note:** The phone ignores URI expansion module key events if the keys are not physically present on the expansion module.
Key:ExpMod2SoftKey1 to Key:ExpMod2SoftKey60	Expansion module 2 soft keys 1 to 60
Key:ExpMod3SoftKey1 to Key:ExpMod3SoftKey60	Expansion module 3 soft keys 1 to 60

Downloaded from www.Manualslib.com manuals search engine

XML Key URI	Description
Volume Key	
Key:VolDwn	Volume Decrease Key
Key:VolUp	Volume Increase Key
Feature Keys	
Key:Xfer	Transfer Key
Key:Conf	Conference Key
Key:Services	Services Key
Key:Intercom	Intercom Key
Key:Headset	Headset Key **Note:** For Headset URI key, the behavior will be as if the "speaker/headset" key is pressed; and does not switch to headset for headset key event or to speaker for speaker key event.
Key:Speaker	Speaker Key **Note:** For Speaker URI key, the behavior will be as if the "speaker/headset" key is pressed; and does not switch to headset for headset key event or to speaker for speaker key event.
Key:Mute	Mute Key
Key:Hold	Hold Key
Key:Redial	Redial Key
Key:Callers	Callers Key
Key:Directory	Directory Key
Key:Options	Options Key
Key:Save	Save Key
Key:Delete	Delete Key
Key:Swap	Swap Key
Key:Goodbye	GoodBye Key
Navigation Keys	
Key:NavUp	Navigation Up Key
Key:NavDwn	Navigation Down Key
Key:NavLeft	Navigation Left Key
Key:NavRight	Navigation Right Key
Function Keys (only if physically configured on the phone or expansion module)	
KeyPark	Park Softkey
KeyPickup	Pickup Softkey

Downloaded from www.Manualslib.com manuals search engine

Notes:
1. If the URI key is a valid key, the phone executes the key regardless of the current state on the phone.
2. Park and Pickup XML URI softkeys are available **ONLY** if these features are physically configured on the phone or expansion module.

Examples

There are two ways to format the XML key URI:

For XML Post Messages

<ExecuteItem URI="<XML Key URI>" />

Example: **<ExecuteItem URI="Key: Line1" />**

For XML Key Scripts

<URI><XML Key URI></URI>

Example: **<URI>Key: Line1</URI>**

```
<SoftKey index="1">
<Label>Keypad1</Label>
<URI>Key: Line1</URI>
</SoftKey>
```


Downloaded from www.Manualslib.com manuals search engine

Using XML Commands to Reset Local Data on the Phone

Release 2.3 provides new XML commands that allow an XML Developer to delete and reset the phone's directory, callers list, redial list, and the *local.cfg* file. You use these commands with the **AastraIPPhoneExecute** object. The following table identifies the new XML commands to reset data on the phone.

XML Command	Description
Command: ClearLocal	• Deletes the *local.cfg* file • Displays a "*Resetting*" message to the IP Phone UI • Resets the phone
Command: ClearCallersList	• Deletes the Callers List • Clears any missed call messages
Command: ClearDirectory	• Deletes the Directory
Command: ClearRedialList	• Deletes the Redial List

Examples

The following examples illustrate the use of the new XML commands to delete and reset data on the phone. The command is shown in bold.

```
<AastraIPPhoneExecute>
   <ExecuteItem URI="Command: ClearLocal"/>
</AastraIPPhoneExecute>

<AastraIPPhoneExecute>
   <ExecuteItem URI="Command: ClearCallersList"/>
</AastraIPPhoneExecute>

<AastraIPPhoneExecute>
   <ExecuteItem URI="Command: ClearDirectory"/>
</AastraIPPhoneExecute>

<AastraIPPhoneExecute>
   <ExecuteItem URI="Command: ClearRedialList"/>
</AastraIPPhoneExecute>
```

Note: The XML commands to reset local data on the phone are not applicable to the Model CT handsets.

Downloaded from www.Manualslib.com manuals search engine

Action URI Disconnected Feature

A new parameter, "**action uri disconnected**" has been added to Release 2.3 that allows a disconnect event to occur when the phone transitions from any active state (outgoing, incoming, connected, or calling) to an idle state. A new line variable called "**$$LINESTATE$$**" has also been added to Release 2.3 that an Administrator can use with the "action uri disconnected" parameter as well as with existing XML URI parameters.

Note: The **$$LINESTATE$$** variable is optional and not required when enabling the "**action uri disconnected**" parameter.

If the Administrator enables this feature (by specifying a disconnect URI), when a call is disconnected, the phone checks to see if the event has a Disconnect URI configured. If the phones finds a configured URI with a $$LINESTATE$$ variable, it replaces the $$LINESTATE$$ variable with the appropriate line state of the current active line. After all of the variables are bound, the phone executes a GET on the URI. The following table lists the applicable values for the $$LINESTATE$$ variable.

$$LINESTATE$$ Value	Description	Meaning in a Disconnected URI
IDLE	Phone is idle.	N/A
DIALING	Phone is offhook and ready to dial.	N/A
CALLING	A SIP INVITE was sent but no response was received.	Error occurred during the call.
OUTGOING	Remote party is ringing.	Call was cancelled.
INCOMING	Local phone is ringing.	Call was missed or cancelled.
CONNECTED	Parties are talking.	Call was successful.
CLEARING	Call was released but not acknowledged.	N/A

The Action URI Disconnect feature allows an Administrator to determine the reason for the disconnect if required.

Note: If you enable the Action URI Disconnect feature by specifying a URI, the URI is called when any disconnect event occurs including an intercom call or a conference setup.

Downloaded from www.Manualslib.com manuals search engine

Example

If you enter the following string on Phone A for the "**action uri disconnected"** parameter:

`action uri disconnected:` **`http://fargo.ana.aastra.com/disconnected.xml?state=$$LINESTATE$$`**

and then Phone A calls Phone B, Phone B answers and then hangs up, Phone A executes a GET on:

`http://fargo.ana.aastra.com/disconnected.xml?state=CONNECTED`

which is what the remote server receives.

Note: If the phone can't find the Action URI you specify, it returns a "NULL" response. For example,
`http://fargo.ana.aastra.com/disconnected.xml?state=`

An Administrator can enable the disconnect feature using the configuration files or the Aastra Web UI.

Configuring the Action URI Disconnect Feature Using the Configuration Files

Use the following parameter to configure the Action URI Disconnect feature.

Parameter– *action uri disconnected*	**Aastra Web UI** Advanced Settings->Action URI->Event **Configuration Files** aastra.cfg, <mac>.cfg
Description	Specifies the URI that the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state. This parameter uses the following variable to determine the state of the line: $$LINESTATE$$
Format	String
Default Value	Blank
Range	Any valid URI
Example	action uri disconnected: http://fargo.ana.aastra.com/disconnected.xml?state=$$LINESTATE$$

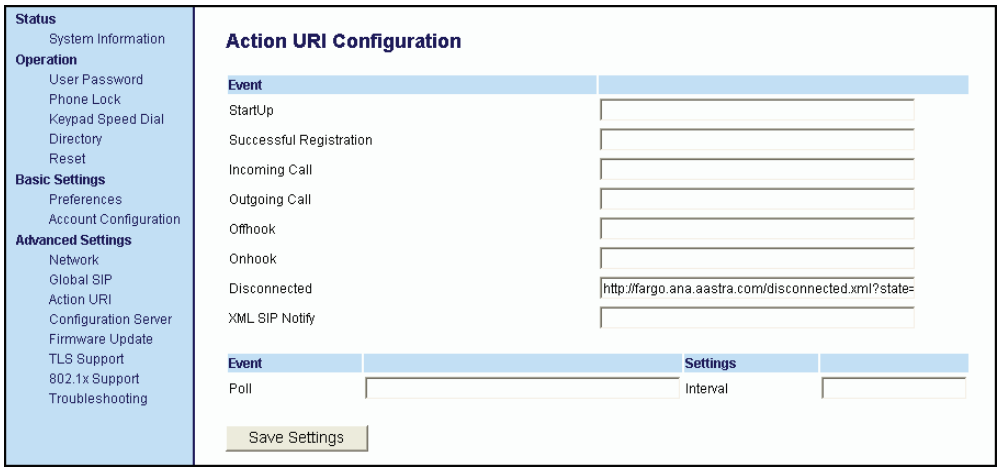
Downloaded from www.Manualslib.com manuals search engine

Configuring the Action URI Disconnect Feature Using the Aastra Web UI

Use the following procedure to configure the Action URI Disconnect feature.

Aastra Web UI

1 Click on **Advanced Settings->Action URI->Event.**



2 In the "**Disconnected**" field, enter a valid URI for which the phone executes a GET on, when it transitions from the incoming, outgoing, calling, or connected state into the idle state. Leaving this field empty disables the Action URI Disconnected feature. For example,

http://fargo.ana.aastra.com/disconnected.xml?state=$$LINESTATE$$

The following table lists the applicable values and descriptions for the $$LINESTATE$$.

$$LINESTATE$$ Value	Description	Meaning in a Disconnected URI
IDLE	Phone is idle.	N/A
DIALING	Phone is offhook and ready to dial.	N/A
CALLING	A SIP INVITE was sent but no response was received.	Error occurred during the call.
OUTGOING	Remote party is ringing.	Call was cancelled.
INCOMING	Local phone is ringing.	Call was missed or cancelled.
CONNECTED	Parties are talking.	Call was successful.
CLEARING	Call was released but not acknowledged.	N/A

3 Click Save Settings to save your settings.

Downloaded from www.Manualslib.com manuals search engine

User Interface Features

Preferred Line Focus Feature

In previous releases of the IP Phones, after a call (incoming or outgoing), the phone would stay on the line that was used for that call. For example, if you made a call on Line 2, then after the call, the display would be showing line 2. Then when you picked up the handset, the phone would go offhook on line 2.

In Release 2.3, an Administrator or User can now define a **preferred line** as well as a **preferred timeout**. If a preferred line is selected, after a call ends (incoming or outgoing), the display switches back to the preferred line. Next time you go off-hook, you pickup on the preferred line. You can specify the number of seconds it takes for the phone to switch back to the preferred line using the "**preferred timeout**" parameter.

An Administrator can configure the "**preferred line**" and the "**preferred timeout**" parameters using the configuration files or the Aastra Web UI. A User can configure these parameters using the Aastra Web UI only.

The following table provides the behavior of the preferred line focus feature with other features on the phone.

Phone Feature	Preferred Line Focus Behavior
call return	The phone switches back to the focused line immediately after the call ends.
speeddial	The line is already specified when the speeddial is created. The phone switches back immediately after the call ends.
conference	For incoming calls, the phone switches back immediately after the call ends.
transfer	For incoming or outgoing calls, the current behavior is that the same line used to transfer the call does not change. For incoming calls, the phone switches back immediately after the call transfers.
blf	The phone switches back immediately after the call ends.
park	The phone switches back immediately after the call ends.
voicemail	The phone switches back immediately after the call ends.
redial	The phone switches back immediately after the call ends.
dialing	For incomplete dialing on a non-preferred line, the focus does not change if some digits are entered. If no digits are entered or digits were cleared, the focus changes to preferred line after the time out has passed without activities.

Downloaded from www.Manualslib.com manuals search engine

Phone Feature	Preferred Line Focus Behavior
caller id	If the "Switch UI Focus To Ringing Line" parameter is disabled, the User is able to see the Caller ID when the phone switches the focus to the ringing line.
factory default	Factory default and recovery mode clears the "preferred line" and "preferred line timeout" parameters, and the phone operates in a non-preferred line mode.

Notes:
1. If you specify a value of "**0**" for the **preferred line** parameter, it disables the preferred line focus feature. The phone behaves as in previous releases.

2. If you specify a value of "**0**" for the **preferred line timeout** parameter, the phone returns the line to the preferred line immediately.

Configuring Preferred Line Focus via the Configuration Files

Use the following parameters to configure preferred line focus using the configuration files.

Parameter– *preferred line* *Preferred Line* (in Web UI)	**Configuration Files** aastra.cfg, <mac>.cfg **Aastra Web UI** Basic Settings->Preferences->General
Description	Specifies the preferred line to switch focus to when incoming or outgoing calls end on the phone.
Format	Integer
Default Value	1
Range	0 (none - disables the preferred line focus feature) 1 to 9
Example	preferred line: 2

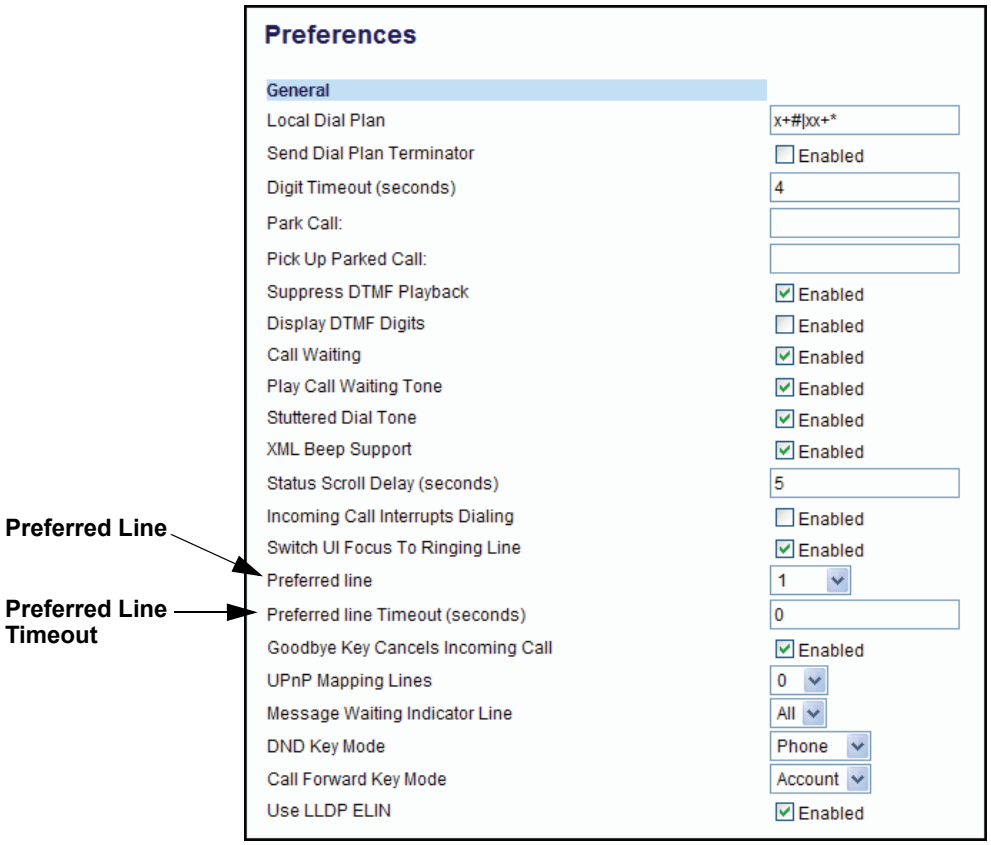
Parameter– *preferred line timeout* *Preferred Line Timeout (seconds)* (in Web UI)	**Configuration Files** aastra.cfg, <mac>.cfg **Aastra Web UI** Basic Settings->Preferences->General
Description	Specifies the time, in seconds, that the phone switches back to the preferred line after a call (incoming or outgoing) ends on the phone, or after a duration of inactivity on an active line.
Format	Integer
Default Value	0 (the phone returns the line to the preferred line immediately)
Range	0 to 999
Example	preferred line timeout: 30

Downloaded from www.Manualslib.com manuals search engine

Configuring Preferred Line Focus via the Aastra Web UI

Use the following parameters to configure preferred line focus using the Aastra Web UI.

Aastra Web UI

1	Click on **Basic Settings->Preferences->General.** 
2	In the "**Preferred Line**" field, select a preferred line to switch focus to after incoming or outgoing calls end on the phone. Valid values are: • **None** (disables the preferred line focus feature) • **1 to 9** Default is **1**. For example, if you set the preferred line to "**1**", when a call (incoming or outgoing) ends on the phone (on any line), the phone switches focus back to Line 1.
3	In the "**Preferred Line Timeout**" field, enter the amount of time, in seconds, that the phone switches back to the preferred line after a call (incoming or outgoing) ends on the phone, or after a duration of inactivity on an active line. Default is **0**. Valid values are: • **0 to 999**
4	Click Save Settings to save your changes.

Downloaded from www.Manualslib.com manuals search engine

Dialpad Speeddial Supported on All Phones

Previously, only the 51i IP Phone supported a dialpad speeddial feature using the IP Phone UI or the Aastra Web UI. In Release 2.3, all the phones now support this feature. Using the IP Phone UI or the Aastra Web UI, an Administrator or User can create speeddial keys on the dialpad.

For more information about speeddial keys, see your model-specific User Guide.

Creating a Speeddial Key using the IP Phone UI

In addition to creating speeddial keys by pressing and holding a key on the keypad, you can also select "**Speed Dial Edit**" at the path *Options->Preferences->Speed Dial Edit*. Use the following procedure to create speeddial keys using the IP Phone UI

You can cancel out of the speeddial editing process at any time without saving, by pressing the key.

Aastra IP Phone UI

Step	Action
1	Press **Options**, and then select **Preferences**. ***On the 51i:*** Press **Services,** and then select **Options->Preferences**.
2	Select **Speed Dial Edit**.
For the 51i (1 line only)	
3	The following prompt displays: "*Press a SD (speeddial) button*".
4	Press any number key on the keypad. For example, "**5**". **Note:** If a number on the keypad is already setup as a speeddial key, pressing the applicable number when creating a speeddial key displays the speeddial information for you to edit. The following prompt displays: "*Enter Number*"
5	Enter the number to assign to this speeddial key and press **SAVE.** **Note:** On the 51i, you can remove the Speeddial Key by erasing the speeddial number digits (leaving the speeddial value blank) and then press SAVE or the RIGHT arrow key. Use the LEFT arrow key to delete the digits. The following prompt displays: "*Saved Memory Key <phone number>*".

Downloaded from www.Manualslib.com manuals search engine

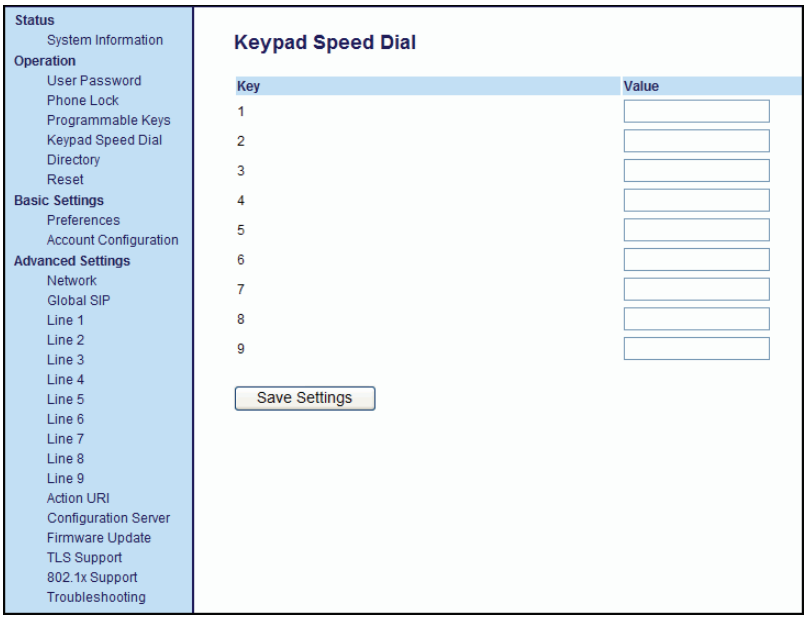
Aastra IP Phone UI

Step	Action
For the 53i and 9143i	
3	The following prompt displays: "*Press a SD (speeddial) button*".
4	Press any number key on the keypad. For example, "**5**". **Note:** If a number on the keypad is already setup as a speeddial key, pressing the applicable number when creating a speeddial key displays the speeddial information for you to edit. The following prompt displays: "*Enter Number"*
5	Enter the number to assign to this speeddial key and press **SAVE.**
6	Select the Line number for which this speeddial dials out on., and press **SAVE**. The following prompt displays: "*Saved Memory Key <phone number>*".
For the 55i, 57i, 57i CT, 9480i, and 9480i CT	
3	The following prompt displays: "*Press a SD (speeddial) button*".
4	Press any number key on the keypad. For example, "**5**". **Note:** If a number on the keypad is already setup as a speeddial key, pressing the applicable number when creating a speeddial key displays the speeddial screen for you to edit. A screen displays allowing you to enter the Name, Number, and Line for which to assign the speeddial key.
5	In the **"Enter Name**" field, enter a name to assign to the speeddial key and press the **DOWN** arrow.
6	In the **"Enter Number**" field, enter a phone number to assign to the speeddial key and press the **DOWN** arrow.
7	In the "**Line**" field, use the **UP** and **DOWN** arrow keys to select a specific line for which the speeddial dials out on.
8	Press **SAVE** to save the changes for the new speeddial key.

Downloaded from www.Manualslib.com manuals search engine

Creating a Speeddial Key using the Aastra Web UI

Use the following procedure to create a speeddial key using the Aastra Web UI.

Aastra Web UI	
1	Click on **Operation->Keypad Speed Dial.** 
2	Choose a key for which to assign a speeddial key. In the "**Value**" field, enter the phone number to assign to the speeddial key.
3	Click to save your changes.

Downloaded from www.Manualslib.com manuals search engine

UTF- 8 Codec for Multi-National Language Support

The IP Phones, expansion modules, and cordless handsets previously supported ISO 8859-1 (Latin1) language. The IP Phones and expansion modules now include support for ISO 8859-2 (Latin2) of multi-national languages when displaying and inputing in the IP Phone UI and the Aastra Web UI.

Note: This feature is not applicable to the handsets on the 57i CT and the 9480i CT.

UTF-8 is also compatible with XML encoding on the IP Phones.

The following table illustrates the Latin 2 character set now used on the IP Phones.

	−0	−1	−2	−3	−4	−5	−6	−7	−8	−9	−A	−B	−C	−D	−E	−F
A−	NBSP 00A0 160	Ą 0104 161	˘ 02D8 162	Ł 0141 163	¤ 00A4 164	Ľ 013D 165	Ś 015A 166	§ 00A7 167	¨ 00A8 168	Š 0160 169	Ş 015E 170	Ť 0164 171	Ź 0179 172	SHY 00AD 173	Ž 017D 174	Ż 017B 175
B−	° 00B0 176	ą 0105 177	˛ 02DB 178	ł 0142 179	´ 00B4 180	ľ 013E 181	ś 015B 182	ˇ 02C7 183	¸ 00B8 184	š 0161 185	ş 015F 186	ť 0165 187	ź 017A 188	″ 02DD 189	ž 017E 190	ż 017C 191
C−	Ŕ 0154 192	Á 00C1 193	Â 00C2 194	Ă 0102 195	Ä 00C4 196	Ĺ 0139 197	Ć 0106 198	Ç 00C7 199	Č 010C 200	É 00C9 201	Ę 0118 202	Ë 00CB 203	Ě 011A 204	Í 00CD 205	Î 00CE 206	Ď 010E 207
D−	Đ 0110 208	Ń 0143 209	Ň 0147 210	Ó 00D3 211	Ô 00D4 212	Ő 0150 213	Ö 00D6 214	× 00D7 215	Ř 0158 216	Ů 016E 217	Ú 00DA 218	Ű 0170 219	Ü 00DC 220	Ý 00DD 221	Ţ 0162 222	ß 00DF 223
E−	ŕ 0155 224	á 00E1 225	â 00E2 226	ă 0103 227	ä 00E4 228	ĺ 013A 229	ć 0107 230	ç 00E7 231	č 010D 232	é 00E9 233	ę 0119 234	ë 00EB 235	ě 011B 236	í 00ED 237	î 00EE 238	ď 010F 239
F−	đ 0111 240	ń 0144 241	ň 0148 242	ó 00F3 243	ô 00F4 244	ő 0151 245	ö 00F6 246	÷ 00F7 247	ř 0159 248	ů 016F 249	ú 00FA 250	ű 0171 251	ü 00FC 252	ý 00FD 253	ţ 0163 254	˙ 02D9 255

Downloaded from www.Manualslib.com manuals search engine

Addition of New Timezone and Country Codes

In Release 2.3, the following new timezones and country codes have been added.

Time Zone Country Code/Time Zone Name	Time Zone Code
AZ - Azerbaijan (Baku)	AZT
GE - Georgia (Tbilisi)	GET
MU - Mauritius	MUT
OM - Oman (Muscat)	GST
AE - United Arab Emirates (Dubai)	GST

Downloaded from www.Manualslib.com manuals search engine

SIP Features

P-Asserted-Identity (PAI) Support in UPDATE message

In previous releases, the IP Phones supported P-Asserted-Identity (PAI). In Release 2.3, the phones now support PAI header in the UPDATE message, according to draft-ietf-sipping-update-pai-00. This feature is always enabled.

If an UPDATE is received with a PAI header from a trusted source, the phone updates the display with this information. The phone ignores any PAI received from untrusted entities.

DTMF Tones in Info Requests

In Release 2.3, the phones now support decoding and playing out DTMF tones sent in SIP INFO requests. The following is now supported:

- Support signals 0-9, #, *
- Support durations up to 5 seconds

Downloaded from www.Manualslib.com manuals search engine

Ignore Out of Sequence Errors

In Release 2.3, an Administrator can configure the phone via the "**sip accept out of order requests**" parameter to ignore CSeq number errors on all SIP dialogs on the phone. When this parameter is enabled, the phone no longer verifies that the sequence numbers increase for each message within a dialog, and does not report a "CSeq Out of Order" error if they do not increase.

Note: As the default Asterisk configuration does not fully track dialogs through a reboot, it is recommended that this parameter be enabled when using the BLF feature with an Asterisk server. If you do not enable this feature, then rebooting the Asterisk server may cause BLF to stop working. With this parameter enabled, the BLF key starts working again when the phone re-subscribes, which by default, are one hour apart.

Enabling/Disabling "Out of Order SIP Requests"

Use the following parameter to enable or disable the SIP out of order requests.BL

Parameter– *sip accept out of order requests*	**Configuration Files** aastra.cfg, <mac>.cfg
Description	Enables a workaround for non-compliant SIP devices (for example, Asterisk) which do not increment the CSeq numbers in SIP requests sent to the phone.
Format	Boolean
Default Value	0 (disabled)
Range	0 (disabled) 1 (enabled)
Example	sip accept out of order requests: 1

Downloaded from www.Manualslib.com manuals search engine

SIP BLA Expires Timer

Release 2.3 now includes a SIP BLA subscription period parameter that allows an Administrator to set the amount of time, in seconds, of the BLA subscription period.

If this parameter is set to zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified in the Subscribe message received from the server, the phone uses the default value of 300 seconds.

You can configure this parameter using the configuration files or the Aastra Web UI.

Configuring SIP BLA Expirey Timer Using the Configuration Files

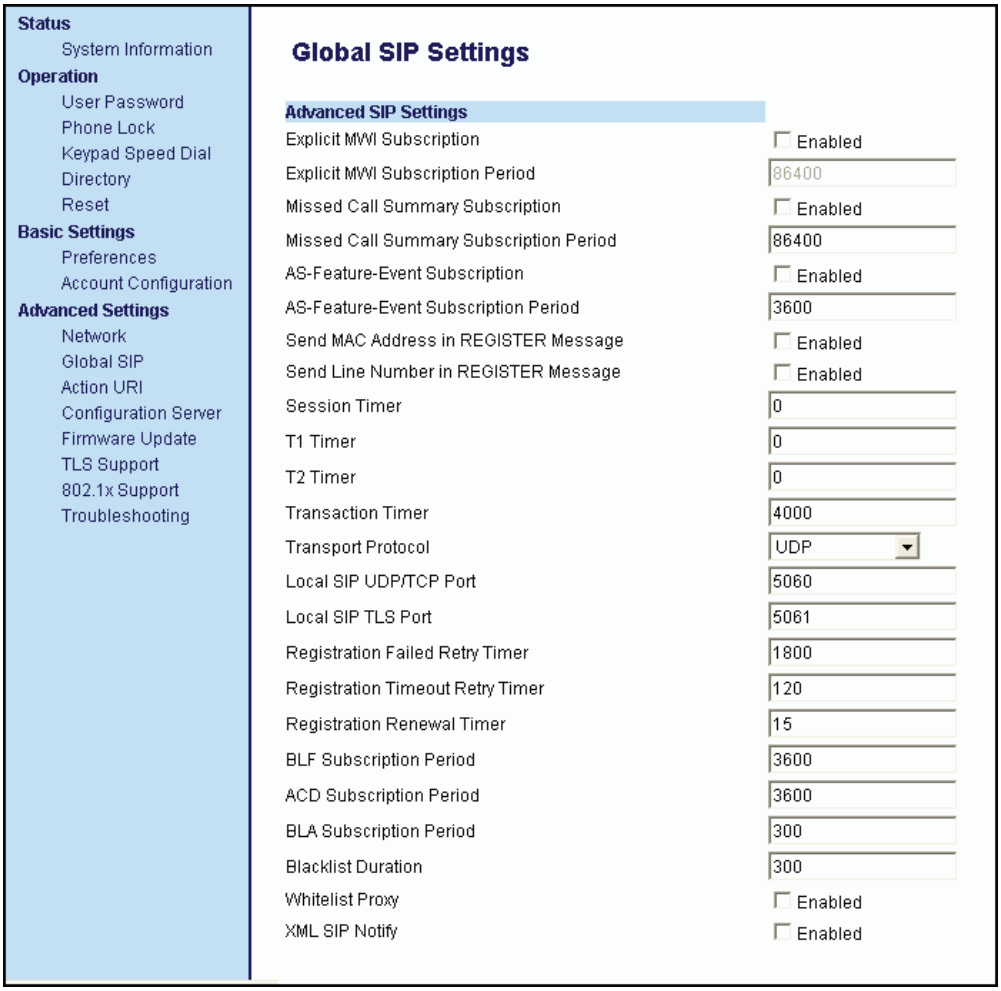
Use the following parameters to configure the BLA expirey timer using the configuration files.

Parameter– *sip bla subscription period* *BLA Subscription Period* (in Web UI)	**Configuration Files** **Aastra Web UI**	aastra.cfg, <mac>.cfg Advanced Settings->Global SIP-> Advanced SIP Settings
Description	Specifies the amount of time, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds.	
Format	Integer	
Default Value	300	
Range	0 to 3700 **Note:** When set to zero (0), the phone uses BLA expiry value specified in subscribe message.	
Example	sip bla subscription period: 0	

Downloaded from www.Manualslib.com manuals search engine

Configuring SIP BLA Expirey Timer Using the Aastra Web UI

Use the following procedure to configure the SIP BLA Subscription Period using the Aastra Web UI.

Aastra Web UI	
1	Click on **Advanced Settings->Global SIP->Advanced SIP Settings.** 
2	In the "**BLA Subscription Period**" field, enter a value, in seconds, that the phone waits to receive a BLA subscribe message from the server. If you specify zero (0), the phone uses the value specified for the BLA expiration in the subscribe message received from the server. If no value is specified, the phone uses the default value of 300 seconds. Valid values are 0 to 3700. Default is 300 seconds.
3	Click Save Settings to save your changes.

Downloaded from www.Manualslib.com manuals search engine

Troubleshooting Features

WatchDog Task Feature

Release 2.3 provides a troubleshooting feature called the "**WatchDog**" task that monitors the status of the phones and provides the ability to get stack traces from the last time the phone failed. When the phone detects a failure (i.e., a crash), it automatically reboots. You can view a WatchDog crash file using the Aastra Web UI at the path, *Advanced Settings->Troubleshooting*. You can enable/disable the WatchDog task using the configuration files or the Aastra Web UI.

Enabling/Disable WatchDog Using the Configuration Files

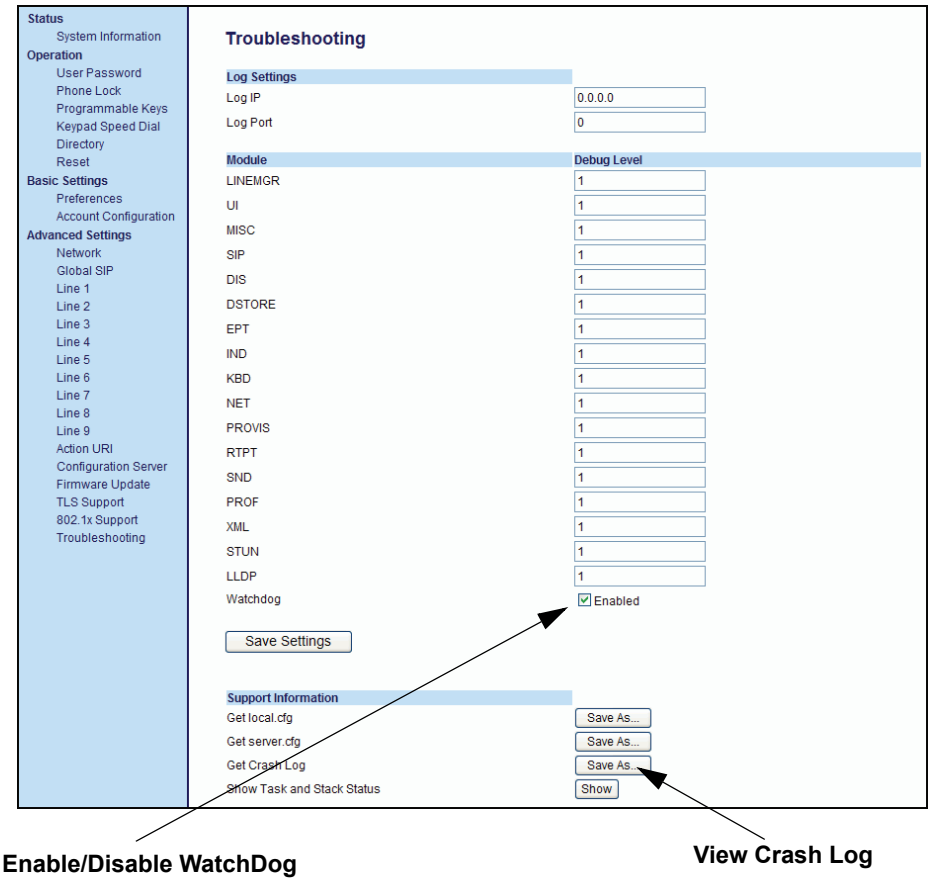
Use the following parameter to enable/disable the WatchDog task for the IP Phones using the configuration files.

Parameter– *watchdog enable* *WatchDog* (in Web UI)	**Configuration Files** **Aastra Web UI**	aastra.cfg, <mac>.cfg Advanced Settings->Troubleshooting
Description	Enables/disables the use of the WatchDog task for the IP Phones.	
Format	Boolean	
Default Value	1 (enabled)	
Range	0 (disabled) 1 (enabled)	
Example	watchdog enable: 0	

Downloaded from www.Manualslib.com manuals search engine

Enabling/Disable WatchDog Using the Aastra Web UI

Use the following procedure to enable/disable the WatchDog task for the IP Phones using the Aastra Web UI. You can also view the "Crash Log" generated by the WatchDog task using the Aastra Web UI.

Aastra Web UI	
1	Click on **Advanced Settings->Troubleshooting.** 
Enable/Disable WatchDog Task	
2	The "**WatchDog**" field is enabled by default. To disable the WatchDog task, click in the "Enabled" box to clear the check mark.
3	Click to save your changes.
View the Crash Log	
4	To view a crash log, in the "**Get a Crash Log**" field, click the **SAVE AS** button. You can open the file immediately, or you can save the Crash Log to your PC.

Downloaded from www.Manualslib.com manuals search engine

Issues Resolved in Release 2.3

This section describes the issues resolved on the 9143i, 9480i, 9480i CT, and the 5i Series IP phones in Release 2.3. The following table provides the issue number and a brief description of each fix.

Note: Unless specifically indicated, these resolved issues apply to all phone models.

Issue Number	Description of Fix
User Interface	
CLN10378	53i: Pickup key now works when there is a held call on the phone.
CLN10430	The TRUN password is no longer displayed in clear text on the WebUI.
ENH08045	Phone now plays DTMF tones it receives via SIP INFO packets.
DEF09452	Lock item is only displayed if both TLS and SRTP are in use.
DEF09517	Dial plan is no longer used after receipt of a 484 Address Incomplete message.
DEF09689	Audible ringback now continues to play if a monitored BLF line changes or an incoming call is received on the phone.
DEF09879	Corrected some German translation errors for the softkeys.
DEF09974	When you are offhook and another call comes in, then the BLF/Xfer and Speeddial/Xfer keys work as speed dials.
DEF10114	Dialed numbers beginning with a * and having a total of three * (eg *8*81*201) are no longer treated like an IP address.
DEF10125	Early media is now played when STUN is enabled.
DEF10236	51i: Dialing numbersfrom the directory that were entered into the directory from the phone now work correctly.
DEF10369	A transferred call (INVITE with replaces) no longer un-mutes the microphone.
XML	
DEF07935	When scrolling quickly through multiple input fields, the phone no longer switches back to the previous screen.
DEF08582	Pressing the right-arrow on a field that is not editable no longer exits the object.
ENH10109	HTTPS URLs are now supported in the XML execute object.
SIP	
DEF07398	SCA: Phone now sends the correct appearance index for conference calls.
DEF08024	BLF: Phone now retries SUBSCRIBE messages more often.
DEF08179	ACD: Incorrect state change messages no longer trigger the phone to change state..
DEF08594	Phone now rejects incoming SRTP calls if SRTP is disabled.
DEF08643	BLA: Phone now sends a terminating NOTIFY when it terminates the subscription
DEF09820	As-feature-sync SUBSCRIBE messages now accept the symmetric sip messaging parameter.
DEF10067	Phone now supports usernames with dots (.)

Downloaded from www.Manualslib.com manuals search engine

Issue Number	Description of Fix
DEF10102	Retry-After headers with additional parameters are now supported.
DEF10323	RTCP packets are no longer treated like early media.
DEF10328	Phone now supports Replaces headers from servers that get the from-tag and to-tag mixed up.
Robustness	
DEF07375	Fixed a crash if you dial a number ending with a # using manual dialling.
DEF09481	Phone now continues to attempt to get DHCP address in the background if it boots up prior to the network being up.
DEF10185	Phone no longer reloads firmware every time it is factory defaulted

Downloaded from www.Manualslib.com manuals search engine

Contacting Aastra Telecom Support

If you've read this release note, and consulted the Troubleshooting section of your phone model's manual and still have problems, please send inquiries via email to beta_support@aastra.com.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Generic SIP IP Phone
Models 9143i, 9480i, 9480i CT, and 5i Series
2.3 Release Notes

Copyright © 2008 Aastra Telecom. All rights reserved. Information in this document is subject to change without notice. Aastra Telecom assumes no responsibility for any errors that may appear in this document. Product capabilities described in this document pertain solely to Aastra Telecom's marketing activities in the U.S. and Canada. Availability in other markets may vary.

RN-001029-02 Rev 00
Release 2.3
June 2008

Downloaded from www.Manualslib.com manuals search engine